

Horizon 7 Upgrades

JUL 2019

VMware Horizon 7 7.9



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2009-2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Horizon 7 Upgrades to 7.9	5
1 Horizon 7 Upgrade Overview	6
2 Applying an Extended Service Branch	9
3 Upgrade the Client Application	10
4 System Requirements for Horizon 7 Server Upgrades	12
Compatibility Matrix for Various Versions of Horizon 7 Components	12
View Composer Requirements	13
Supported Operating Systems for View Composer	13
Hardware Requirements for Standalone View Composer	14
Upgrade Requirements for View Composer	14
Horizon Connection Server Requirements	15
Hardware Requirements for Horizon Connection Server	15
Supported Operating Systems for Horizon Connection Server	16
Upgrade Requirements for Horizon Connection Server	16
Supported Operating Systems for Horizon Agent	18
5 Upgrading Horizon 7 Server Components	19
Upgrading View Composer	19
Preparing vCenter Server and View Composer for an Upgrade	20
Upgrade View Composer	21
Enable TLSv1.0 on vCenter and ESXi Connections from View Composer	22
Enable Digest Access Authentication for View Composer	23
Manually Upgrading the View Composer Database	24
Migrate View Composer to Another Machine	27
Upgrading Horizon Connection Server	34
Preparing Connection Server for an Upgrade	34
Upgrade Connection Servers in a Replicated Group	35
Enable TLSv1.0 on vCenter Connections from Connection Server	38
Upgrade to the Latest Version of Connection Server on a Different Machine	39
Create a Replicated Group After Reverting Connection Server to a Snapshot	40
Upgrading Security Servers	41
Preparing Security Server for an Upgrade	42
Upgrade Security Servers and Their Paired Connection Servers	42
Replacing a Security Server with a Unified Access Gateway Appliance	45

Upgrading a Cloud Pod Architecture Environment	46
Upgrading Horizon 7 Servers to Allow HTML Access	47
Upgrade vCenter Server	47
Accept the Thumbprint of a Default TLS Certificate	48
Using Horizon 7 Group Policy Administrative Template Files	50

6 Upgrade ESXi Hosts and Their Virtual Machines 52

7 Upgrading Published and Virtual Desktops 55

Security-Related Requirements for Desktop Upgrade	55
Upgrade RDS Hosts That Provide Session-Based Desktops	55
Upgrade View Agent or Horizon Agent	57
Upgrade View Composer Desktop Pools	59
Upgrade Instant-Clone Desktop Pools	61

8 Upgrade Horizon 7 Cloud Connector Virtual Appliance 63

Static IP and Proxy Configuration for the Horizon 7 Cloud Connector Virtual Appliance	65
Update the Static IP for the Horizon 7 Cloud Connector Virtual Appliance	66
Troubleshoot the Horizon 7 Cloud Connector Virtual Appliance Upgrade	66

9 Post-Upgrade Tasks to Enable New Features in Your Horizon Setup 68

Change the JMS Message Security Mode to Enhanced	68
Tasks for Upgrading Desktop Pools to Use Space Reclamation	69
Upgrade Tasks If You Use VMware vSAN Datastores	71
Upgrade from a Non-vSAN Datastore to a vSAN Datastore	71
Upgrade from vSAN Disk Format Version 1	72
Upgrade from Horizon View 5.3.x on a vSAN Datastore	74
Configure the VMware Horizon Web Portal Page for End Users	75

10 Upgrading vSphere Components Separately in a Horizon 7 Environment 80

Horizon 7 Upgrades to 7.9

Horizon 7 Upgrades provides instructions for upgrading from the latest maintenance releases of Horizon View 5.3, VMware Horizon™ 6 (with View), or VMware Horizon 6 version 6.1 or 6.2, to VMware Horizon 7. You can also use this guide when you upgrade to Horizon 7 maintenance releases.

If you are also upgrading your version of VMware vSphere®, this guide tells you which steps of that upgrade to do at various stages of the Horizon 7 upgrade.

Intended Audience

This guide is intended for anyone who needs to upgrade to this latest version of this product. The information in this guide is written for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Horizon 7 Upgrade Overview

Upgrading an enterprise Horizon 7 deployment involves several high-level tasks. Upgrading is a multistage process in which procedures must be performed in a particular order. You upgrade View Composer before upgrading Horizon Connection Server and the other Horizon 7 servers.

Important With Horizon 6 version 6.2 and later versions, you can install Horizon 7 components to run in FIPS mode. Horizon 7 does not support upgrading from a non-FIPS installation to a FIPS installation. Horizon does support upgrading from Horizon 6 version 6.2 in FIPS mode to Horizon 7 in FIPS mode. If you need to do a fresh installation, see "Installing Horizon 7 in FIPS Mode," in the *Horizon 7 Installation* document.

During an upgrade, Horizon 7 does not support View Composer provisioning and maintenance operations. Operations such as provisioning and recomposing linked-clone desktops are not supported during the transitional period when any Horizon 7 servers are still running the earlier version. You can successfully perform these operations only when all instances of Connection Server and View Composer have been upgraded.

You must complete the upgrade process in a specific order. Order is also important within each upgrade stage.

Note This overview relates to upgrades for major, minor, and maintenance releases.

How many of the following tasks you need to complete depends on which components of Horizon 7 you use in your deployment.

- 1 Upgrade the Horizon Client software that runs on end users' client devices. See [Chapter 3 Upgrade the Client Application](#).
- 2 On the physical or virtual machines that host View Composer and VMware® vCenter Server™, make backups and temporarily halt certain scheduled tasks. See [Preparing vCenter Server and View Composer for an Upgrade](#).

If you have a standalone View Composer, which is installed in a separate machine from vCenter Server, you need only make a backup of the View Composer database and the View Composer TLS/SSL certificate. You can schedule an upgrade of vCenter Server separately, if you want to also upgrade vCenter Server.

For details about which versions of Horizon are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- 3 Upgrade View Composer on the existing host or migrate to a new machine. See [Upgrade View Composer](#).
- 4 On the physical or virtual machines that host Connection Server instances, make backups and record various configuration and system settings. See [Preparing Connection Server for an Upgrade](#).

If you have multiple Connection Server instances in a replicated group, make backups and record configuration settings for only one instance in the group. For other preparation tasks, you can perform the tasks for one instance at a time, just before you perform the upgrade of that server instance.

- 5 Upgrade Connection Server instances that are not paired with security servers. See [Upgrade Connection Servers in a Replicated Group](#).

In a typical production environment that consists of two or more Connection Server instances fronted by a load balancer, if you need to minimize down time, you can remove Connection Server instances from the load balanced cluster one at a time while you upgrade them.

Important After you upgrade a Connection Server instance to the latest version, you cannot downgrade that instance to an earlier version. After you upgrade all Connection Server instances in a replicated group, you cannot add another instance that runs an earlier version.

- 6 If you use security servers, make backups and record various configuration and system settings. See [Preparing Security Server for an Upgrade](#).

To minimize down time, you can perform these tasks for one security server at a time, just before you perform the upgrade of that server.

- 7 If you use security servers, upgrade each security server and its paired Connection Server instance. If you upgrade these pairs one by one, removing each security server from the load-balanced group, upgrading the pair, and then adding the security server back to the group, you can achieve zero downtime. See [Upgrade Security Servers and Their Paired Connection Servers](#).

- 8 Upgrade the group policies used in Active Directory. See [Using Horizon 7 Group Policy Administrative Template Files](#).

- 9 If you are also upgrading VMware vSphere components, upgrade vCenter Server. See [Upgrade vCenter Server](#).

During the vCenter Server upgrade, existing remote desktop and application sessions will not be disconnected. Remote desktops that are in a provisioning state will not get powered on during the vCenter Server upgrade, and new desktops cannot be launched and View Composer operations are not allowed during the vCenter Server upgrade.

- 10 If you are also upgrading vSphere, upgrade the VMware[®] ESXi[™] hosts and virtual machines. See [Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines](#).

ESXi hosts can be upgraded with zero down time by vMotioning the virtual machines to another host in the cluster, if hosts are configured under clustered environment.

- 11 If you currently use Windows Terminal Services servers as desktop sources, upgrade to Windows Server 2008 R2 or later and verify that the RDS Host role is installed. See [Upgrade RDS Hosts That Provide Session-Based Desktops](#)

- 12 Upgrade the Horizon™ Agent or View Agent™ software that runs on the physical or virtual machines that are used as desktop sources, as full-clone desktops in a pool, and as individual desktops in a manual pool. See [Upgrade View Agent or Horizon Agent](#).
- 13 Use the newly upgraded virtual machine desktop sources to create upgraded pools of desktops. See [Upgrade View Composer Desktop Pools](#).
- 14 If you use the Cloud Pod Architecture feature, see [Upgrading a Cloud Pod Architecture Environment](#).

Because certain commands can simultaneously upgrade more than one stage, VMware recommends that you thoroughly understand the irreversible changes at each stage before you upgrade your production environments.

Important The VMware View® Client with Local Mode feature, for using offline desktops, has been removed, and therefore this overview does not include steps for upgrading View Transfer Server instances and View Client with Local Mode. In place of the Local Mode feature, VMware recommends using VMware® Mirage™, which is included with VMware Horizon 6.0 and later releases. For more information, see the Horizon 7 Release Notes, available at <https://docs.vmware.com/en/VMware-Horizon-7/index.html>.

Applying an Extended Service Branch

2

An Extended Service Branch (ESB) is an option available starting with Horizon 7.5, VMware App Volumes 2.14, and VMware User Environment Manager 9.4.0. It contains periodic service pack (SP) updates, which include cumulative, critical bug fixes, and security fixes.

If you decide not to upgrade to the latest version of Horizon, and instead remain on the same version, you can deploy an ESB and continue to receive timely bug and security fixes. The SP updates do not include new features, so you can rely on a stable Horizon platform for your critical deployments.

Separate ESBs are available once a year for the core Horizon platform, VMware App Volumes, and VMware User Environment Manager. ESBs are supported for 24 months with three scheduled SP updates: SP1 will be released six months after the initial release, SP2 will be released three months after SP1, and SP3 will be released six months after SP2.

For more information, see FAQ: Horizon 7, App Volumes, UEM Extended Service Branches (ESB) <https://kb.vmware.com/s/article/52845>.

Upgrade the Client Application

Upgrade to the latest version of Horizon Client and upgrade the firmware on thin client devices if you use them.

The Local Mode feature for Horizon Client has been removed. In its place, VMware recommends using Mirage, which is included with VMware Horizon 7. For more information, see the Horizon 7 Release Notes, available at <https://docs.vmware.com/en/VMware-Horizon-7/index.html>.

Important Upgrading involves running the new version of the Horizon Client installer without first removing the older version of the client application. If your end users have the Windows-based View Client 4.6.0 or an earlier version, instruct them to remove the client software before downloading and running the latest Horizon Client installer.

Prerequisites

- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- Verify that the client desktop, laptop, tablet, or phone meets the operating system requirements and hardware requirements of Horizon Client. See the "Using Horizon Client" document for the specific type of desktop or mobile client device. Go to <https://docs.vmware.com/en/VMware-Horizon-Client/index.html>.

Procedure

- 1 Have end users upgrade to the latest version of Horizon Client.

Option	Action
Horizon Client	<p>Download and send the Horizon Client installers to your end users or post them on a Web site and ask end users to download the installer and run it. You can download the installers or have your end users download them from the VMware Web site at https://www.vmware.com/go/viewclients.</p> <p>For mobile clients, you can alternatively instruct your end users to get the latest version of Horizon Client from other Web sites that sell apps, including the Apple App Store, Google Play, Amazon, and Windows Store.</p>
VMware Horizon user Web portal	<p>End users can open a browser and browse to a Connection Server instance. The Web page that appears is called the VMware Horizon user Web portal, and it contains links for downloading the installer file for Horizon Client.</p> <p>Note The default links in Web page point to the Horizon Client download site. You can change the default links to point elsewhere. See Configure the VMware Horizon Web Portal Page for End Users.</p>
Thin client	<p>Upgrade the thin client firmware and install the new Horizon Client software on end users' client devices. Thin clients and zero clients are provided by VMware partners.</p>

- 2 Have end users verify that they can log in and connect to their remote desktops.

System Requirements for Horizon 7 Server Upgrades

4

Hosts and virtual machines in a Horizon 7 deployment must meet specific hardware and operating system requirements.

This chapter includes the following topics:

- [Compatibility Matrix for Various Versions of Horizon 7 Components](#)
- [View Composer Requirements](#)
- [Horizon Connection Server Requirements](#)
- [Supported Operating Systems for Horizon Agent](#)

Compatibility Matrix for Various Versions of Horizon 7 Components

Because large enterprises must often perform phased upgrades, components are designed to be somewhat forward and backward compatible, at least during upgrades.

The following versions are supported for upgrading to Horizon 7:

- Latest maintenance release of Horizon View 5.3
- Latest maintenance release of VMware Horizon 6.0 (with View)
- Latest maintenance release of VMware Horizon 6 version 6.1
- Latest maintenance release of VMware Horizon 6 version 6.2

To determine the latest maintenance release of a particular component, see the Release Notes for that release, available from <https://docs.vmware.com/en/VMware-Horizon-7/index.html>

Horizon Connection Server compatibility with Horizon Agents is limited to interoperability during a Connection Server upgrade. You must upgrade View Agents or Horizon Agents as soon as possible to match the version of the Connection Server that manages them.

The following table lists the components and show whether they are compatible with other components whose version is different.

Table 4-1. Compatibility Matrix for VMware Horizon 7 and Earlier Versions of View Components

	Connection Server: Earlier Version	Security Server: Earlier Version	View Composer: Earlier Version	View Agent: Earlier Version	Horizon Client (Windows): Earlier Version
Connection Server 7.0	Only during upgrade	Only if paired before upgrade	No	Only during upgrade	Yes
Security Server 7.0 (PCoIP and RDP)	No	N/A	No	Only during upgrade	Yes
View Composer 7.0	Only during upgrade	Only during upgrade	N/A	Only during upgrade	N/A
Horizon Agent 7.0	Only during upgrade (see the exception in the note following this table)	No	No	N/A	Only during upgrade
Horizon Client 4.0	Yes	Yes	Yes	Yes	N/A

Caution During an upgrade, View Composer provisioning and maintenance operations are not supported. Operations such as provisioning and recomposing linked-clone desktops are not supported during the transitional period when any Horizon 7 servers are still running the earlier version. You can successfully perform these operations only when all instances of Connection Server and View Composer have been upgraded to the latest version.

For details about which versions of Horizon are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

View Composer Requirements

With View Composer, you can deploy multiple linked-clone desktops from a single centralized base image. View Composer has specific installation and storage requirements.

Supported Operating Systems for View Composer

View Composer supports 64-bit operating systems with specific requirements and limitations. You can install View Composer on the same physical or virtual machine as vCenter Server or on a separate server.

Table 4-2. Operating System Support for View Composer

Operating System	Version	Edition
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise Datacenter
Windows Server 2012 R2	64-bit	Standard Datacenter
Windows Server 2016	64-bit	Standard Datacenter

Note Windows Server 2008 R2 with no service pack is no longer supported.

If you plan to install View Composer on a different physical or virtual machine than vCenter Server, see [Hardware Requirements for Standalone View Composer](#).

Hardware Requirements for Standalone View Composer

If you install View Composer on a different physical or virtual machine from the one used for vCenter Server, you must use a dedicated machine that meets specific hardware requirements.

A standalone View Composer installation works with vCenter Server installed on a separate Windows Server machine or with the Linux-based vCenter Server appliance. VMware recommends having a one-to-one mapping between each View Composer service and vCenter Server instance.

Table 4-3. View Composer Hardware Requirements

Hardware Component	Required	Recommended
Processor	1.4 GHz or faster Intel 64 or AMD 64 processor with 2 CPUs	2GHz or faster and 4 CPUs
Networking	One or more 10/100Mbps network interface cards (NICs)	1Gbps NICs
Memory	4GB RAM or higher	8GB RAM or higher for deployments of 50 or more remote desktops
Disk space	40GB	60GB

Important The physical or virtual machine that hosts View Composer must have an IP address that does not change. In an IPv4 environment, configure a static IP address. In an IPv6 environment, machines automatically get IP addresses that do not change.

Upgrade Requirements for View Composer

The View Composer upgrade process has specific requirements and limitations.

To run the View Composer installer, you must be a domain user with Administrator privileges on the system.

Security-Related Requirements

- View Composer requires a TLS certificate that is signed by a CA (certificate authority). If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate after you install View Composer, you must import the new certificate and run the SviConfig ReplaceCertificate utility to bind your new certificate to the port used by View Composer.

If you install vCenter Server and View Composer on the same Windows Server computer, they can use the same TLS certificate, but you must configure the certificate separately for each component.

For complete information about security certificate requirements, see "Configuring SSL Certificates for View Servers" in the *Horizon 7 Installation* document.

- Certificates for vCenter Server, View Composer, and Horizon 7 servers must include certificate revocation lists (CRLs). For more information, see "Configuring Certificate Revocation Checking on Server Certificates" in the *Horizon 7 Installation* guide.
- Verify that no applications that run on the View Composer computer use Windows SSL libraries that require SSLv2 provided through the Microsoft Secure Channel (Schannel) security package. The View Composer installer disables SSLv2 on the Microsoft Schannel. Applications such as Tomcat, which uses Java SSL, or Apache, which uses OpenSSL, are not affected by this constraint. SSLv3, TLSv1.0, and RC4 are also disabled by default. For more information, see "Older Protocols and Ciphers Disabled in View" in the *Horizon 7 Security* document.
- To enhance the security of View Composer, disable the weak cryptographic cipher suites on the Windows Server computer on which the View Composer service is installed. See "Disable Weak Ciphers in SSL/TLS" in the *Horizon 7 Installation* document.
- You might need to make security protocol configuration changes to continue to be compatible with vSphere. If possible, apply patches to ESXi and vCenter Server to support TLSv1.1 and TLSv1.2 before upgrading View Composer. If you cannot apply patches, reenables TLSv1.0 on View Composer before upgrading. For more information, see [Enable TLSv1.0 on vCenter and ESXi Connections from View Composer](#).
- Effective in Horizon 7 version 7.0.3, you can enable digest access authentication for View Composer to enhance security. For more information, see [Enable Digest Access Authentication for View Composer](#).

Horizon Connection Server Requirements

Horizon Connection Server acts as a broker for client connections by authenticating and then directing incoming user requests to the appropriate remote desktops and applications. Horizon Connection Server has specific hardware, operating system, installation, and supporting software requirements.

Hardware Requirements for Horizon Connection Server

You must install all Horizon Connection Server installation types, including standard, replica, security server, and enrollment server installations, on a dedicated physical or virtual machine that meets specific hardware requirements.

Table 4-4. Horizon Connection Server Hardware Requirements

Hardware Component	Required	Recommended
Processor	Pentium IV 2.0GHz processor or higher	4 CPUs
Network Adapter	100Mbps NIC	1Gbps NICs
Memory Windows Server 2008 R2 64-bit	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more remote desktops
Memory Windows Server 2012 R2 64-bit	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more remote desktops

These requirements also apply to replica and security server Horizon Connection Server instances that you install for high availability or external access.

Important The physical or virtual machine that hosts Horizon Connection Server must have an IP address that does not change. In an IPv4 environment, configure a static IP address. In an IPv6 environment, machines automatically get IP addresses that do not change.

Supported Operating Systems for Horizon Connection Server

You must install Horizon Connection Server on a supported Windows Server operating system.

The following operating systems support all Horizon Connection Server installation types, including standard, replica, and security server installations.

Table 4-5. Operating System Support for Horizon Connection Server

Operating System	Version	Edition
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise Datacenter
Windows Server 2012 R2	64-bit	Standard Datacenter
Windows Server 2016	64-bit	Standard Datacenter
Windows Server 2019	64-bit	Standard Datacenter

Note Windows Server 2008 R2 with no service pack is no longer supported.

Upgrade Requirements for Horizon Connection Server

The Horizon Connection Server upgrade process has specific requirements and limitations.

- Connection Server requires a valid license key for this latest release.

- The domain user account that you use to install the new version of Connection Server must have administrative privileges on the Connection Server host. The Connection Server administrator must have administrative credentials for vCenter Server.
- When you run the installer, you authorize an Administrators account. You can specify the local Administrators group or a domain user or group account. Horizon 7 assigns full Horizon Administration rights, including the right to install replicated Connection Server instances, to this account only. If you specify a domain user or group, you must create the account in Active Directory before you run the installer.
- When you back up Connection Server, the View LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup Horizon 7 configuration, you must provide the data recovery password. The password must contain between 1 and 128 characters.

Security-Related Requirements

- Connection Server requires a TLS certificate that is signed by a CA (certificate authority) and that your clients can validate. Although a default self-signed certificate is generated in the absence of a CA-signed certificate when you install Connection Server, you must replace the default self-signed certificate as soon as possible. Self-signed certificates are shown as invalid in Horizon Administrator.

Also, updated clients expect information about the server's certificate to be communicated as part of the TLS handshake between client and server. Often updated clients do not trust self-signed certificates.

For complete information about security certificate requirements, see "Configuring TLS Certificates for Horizon 7 Servers" in the *Horizon 7 Installation* guide. Also see the *Scenarios for Setting Up TLS Certificates for Horizon 7* document, which describes setting up intermediate servers that perform tasks such as load balancing and off-loading SSL connections.

Note If your original servers already have TLS certificates signed by a CA, during the upgrade, Horizon 7 imports your existing CA-signed certificate into the Windows Server certificate store.

- Certificates for vCenter Server, View Composer, and Horizon 7 servers must include certificate revocation lists (CRLs). For more information, see "Configuring Certificate Revocation Checking on Server Certificates" in the *Horizon 7 Installation* document.

Important If your company uses proxy settings for Internet access, you might have to configure your Connection Server hosts to use the proxy. This step ensures that servers can access certificate revocation checking sites on the Internet. You can use Microsoft Netshell commands to import the proxy settings to Connection Server. For more information, see "Troubleshooting Horizon 7 Server Certificate Revocation Checking" in the *Horizon 7 Administration* document.

- If you plan to pair a security server with this Connection Server instance, verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and Connection Server and require Windows Firewall with Advanced Security to be enabled.

- If your network topology includes a firewall between a security server and a Connection Server instance, you must configure the firewall to support IPsec. See the *Horizon 7 Installation* document.
- You might need to make security protocol configuration changes to continue to be compatible with vSphere. If possible, apply patches to ESXi and vCenter Server to support TLSv1.1 and TLSv1.2 before upgrading Connection Server. If you cannot apply patches, reenabling TLSv1.0 on Connection Server before upgrading. For more information, see [Enable TLSv1.0 on vCenter Connections from Connection Server](#).
- If you use Horizon 7 servers with a version of View Agent older than 6.2, you will need to enable TLSv1.0 for PCoIP connections. View Agent versions that are older than 6.2 support the security protocol TLSv1.0 only for PCoIP. Horizon 7 servers, including connection servers and security servers, have TLSv1.0 disabled by default. You can enable TLSv1.0 for PCoIP connections on these servers by following the instructions in the VMware Knowledge Base, at <http://kb.vmware.com/kb/2130798>.

If you plan to perform fresh installations of Connection Server instances on additional physical or virtual machines, see the complete list of installation requirements in the *Horizon 7 Installation* document.

Supported Operating Systems for Horizon Agent

The Horizon Agent component (called View Agent in previous releases) assists with session management, single sign-on, device redirection, and other features. You must install Horizon Agent on all virtual machines, physical systems, and RDS hosts.

The types and editions of the supported guest operating system depend on the Windows version. For updates to the list of supported Windows 10 operating systems, see the VMware Knowledge Base (KB) article <http://kb.vmware.com/kb/2149393>. For Windows operating systems other than Windows 10, see the VMware Knowledge Base (KB) article <http://kb.vmware.com/kb/2150295>.

To see a list of specific remote experience features supported on Windows operating systems where Horizon Agent is installed, see the VMware Knowledge Base (KB) article <http://kb.vmware.com/kb/2150305>.

For enhanced security, VMware recommends configuring cipher suites to remove known vulnerabilities. For instructions on how to set up a domain policy on cipher suites for Windows machines that run View Composer or Horizon Agent, see the topic about disabling weak ciphers for View Composer or Horizon Agent in the *Horizon 7 Installation* document.

Upgrading Horizon 7 Server Components

5

The server components that you must upgrade include Horizon Connection Server, replicated servers, and security servers. Depending on the optional components you use, you might also need to upgrade View Composer.

If you spread the upgrade tasks across multiple maintenance windows, you can verify success or discover issues at each phase of the process. VMware recommends upgrading all server components during the first maintenance window.

This chapter includes the following topics:

- [Upgrading View Composer](#)
- [Upgrading Horizon Connection Server](#)
- [Upgrading Security Servers](#)
- [Upgrading a Cloud Pod Architecture Environment](#)
- [Upgrading Horizon 7 Servers to Allow HTML Access](#)
- [Upgrade vCenter Server](#)
- [Accept the Thumbprint of a Default TLS Certificate](#)
- [Using Horizon 7 Group Policy Administrative Template Files](#)

Upgrading View Composer

During an upgrade, Horizon 7 does not support View Composer provisioning and maintenance operations. Operations such as provisioning and recomposing linked-clone desktops are not supported during the transitional period when any Horizon 7 servers are still running the earlier version. You can successfully perform these operations only when all instances of Horizon Connection Server and View Composer have been upgraded.

Note Before you can use the View Composer 6.2 feature for creating automated farms of linked-clone RDS hosts, you must upgrade all Horizon components to Horizon 6 version 6.2 or later.

Preparing vCenter Server and View Composer for an Upgrade

Because vCenter Server and View Composer are often installed on the same virtual or physical machine, some preparation tasks apply to both.

Preparing for Upgrades That Include vSphere

If you are upgrading vCenter Server in addition to upgrading to the latest version of Horizon 7, you must consult the *VMware vSphere Upgrade Guide* and perform the following tasks in the following order:

- 1 Verify that the virtual or physical machine meets the system requirements for the version of vCenter Server that you want to upgrade to.
- 2 Verify that the virtual or physical machine on which the current View Composer is installed meets the security requirements for the new version.

See [Upgrade Requirements for View Composer](#).

- 3 If vCenter Server is installed in a virtual machine, take a snapshot of the virtual machine.
For instructions on taking snapshots, see the vSphere Client™ online help.
- 4 If the computer name is longer than 15 characters, shorten the name to 15 or fewer characters.
- 5 Back up the vCenter Server database and the View Composer database.

For instructions on performing a database backup, see the documentation from your database vendor.

- 6 Verify that the database server is compatible with the version of vCenter Server you plan to use.
For example, if the database server is Oracle 9i, you must upgrade.

- 7 Verify that the database is compatible with the new version of View Composer.

View Composer supports a subset of the database servers that vCenter Server supports. If you are already using vCenter Server with a database server that is not supported by View Composer, continue to use that database server for vCenter Server and install a separate database server to use for View Composer and Horizon 7 database events.

- 8 Make a copy of the folder that contains TLS certificates.

This folder is located at %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter.

- 9 Document the IP address and system name of the machine on which vCenter Server is installed.
- 10 For all linked-clone and instant-clone desktop pools, use Horizon Administrator to disable provisioning of new virtual machines.

For linked-clones, because View Composer might be upgraded during a different maintenance window than its desktop pools, provisioning must be postponed until both components are upgraded.

- 11 If any linked-clone desktop or instant-clone desktop pools are set to refresh the OS disk on logoff, use Horizon Administrator to edit the **Desktop/Pools** settings for that pool and set **Delete or refresh machine on logoff** to **Never**.

For linked-clones, this setting prevents an error from occurring when the newly upgraded View Composer attempts to refresh a desktop on which Horizon Agent has not yet been upgraded.

- 12 If any linked-clone or instant-clone desktop pools are scheduled to do a refresh, recompose, or image push operation, use Horizon Administrator to cancel these tasks.

Preparing for Upgrades of View Composer Only

If you are upgrading only View Composer and are not upgrading vCenter Server, you must perform the following tasks:

- 1 Verify that the virtual or physical machine on which the current View Composer is installed meets the security requirements for the new version.

See [Upgrade Requirements for View Composer](#).

- 2 If View Composer is installed in a virtual machine, take a snapshot of the virtual machine.

For instructions on taking snapshots, see the vSphere Client online help.

- 3 Back up the View Composer database.

For instructions on performing a database backup, see the documentation from your database vendor.

- 4 Verify that the database is compatible with the new version of View Composer.

View Composer supports a subset of the database servers that vCenter Server supports. If you are already using vCenter Server with a database server that is not supported by View Composer, continue to use that database server for vCenter Server and install a separate database server to use for View Composer and Horizon 7 database events.

- 5 Document the IP address and system name of the machine on which vCenter Server is installed.

- 6 For all linked-clone desktop pools, use Horizon Administrator to disable provisioning of new virtual machines.

Because View Composer might be upgraded during a different maintenance window than its desktop pools, provisioning must be postponed until both components are upgraded.

- 7 If any desktop pools are set to refresh the OS disk on logoff, use Horizon Administrator to edit the **Desktop/Pools** settings for that pool and set **Delete or refresh machine on logoff** to **Never**.

This setting prevents an error from occurring when the newly upgraded View Composer attempts to refresh a desktop on which View Agent has not yet been upgraded.

- 8 If any desktop pools are scheduled to do a refresh or recompose operation, use Horizon Administrator to cancel these tasks.

Upgrade View Composer

During the first maintenance window, you will upgrade View Composer. Operations such as provisioning and recomposing linked-clone desktops are not supported until all Horizon 7 servers are upgraded.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour.
- Complete the tasks listed in [Preparing for Upgrades of View Composer Only](#).
- Verify that the server on which View Composer is installed has a CA (certificate authority)-signed TLS/SSL server certificate installed and configured. After you upgrade Horizon Connection Server, if View Composer does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in Horizon Administrator.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- Determine whether to let the installer wizard upgrade the View Composer database if a schema upgrade is required. You can choose to run the SviConfig command-line utility after the wizard finishes to upgrade the database schema manually and to create a log of the upgrade.

Procedure

- 1 On the virtual or physical machines where View Composer is installed, download and run the installer for View Composer.

You can download the installer from the VMware Web site.

Step-by-step instructions for running the installer appear in the *Horizon 7 Installation* document.

- 2 Specify whether you want the wizard to upgrade the database schema if a schema upgrade is required.

If a dialog box appears with the message "Database upgrade completed with warnings" you can click **OK** and safely ignore the message.

- 3 When the wizard prompts you for the View Composer port number, verify that the port number is set to 18443.

What to do next

If you need to do a manual upgrade of the database schema, see [Run SviConfig to Manually Upgrade the Database](#).

If you have an older version of vCenter Server, see [Enable TLSv1.0 on vCenter and ESXi Connections from View Composer](#).

At your next maintenance window, continue with the Horizon 7 upgrade. See [Upgrade Connection Servers in a Replicated Group](#).

Enable TLSv1.0 on vCenter and ESXi Connections from View Composer

Horizon 7 and later components have the TLSv1.0 security protocol disabled by default. If your deployment includes an older version of vCenter Server that supports only TLSv1.0, you might need to

enable TLSv1.0 for View Composer connections after installing or upgrading to View Composer 7.0 or a later release.

Some earlier maintenance releases of vCenter Server 5.0, 5.1, and 5.5 support only TLSv1.0, which is no longer enabled by default in Horizon 7 and later releases. If it is not possible to upgrade vCenter Server to a version that supports TLSv1.1 or TLSv1.2, you can enable TLSv1.0 for View Composer connections.

If your ESXi hosts are not running ESXi 6.0 U1b or later, and you cannot upgrade, you might also need to enable TLSv1.0 connections to ESXi hosts from View Composer.

Prerequisites

- Verify that you have View Composer 7.0 or a later release installed.
- Verify that you can log in to the View Composer machine as an Administrator to use the Windows Registry Editor.

Procedure

- 1 On the machine that hosts View Composer, open the Windows Registry Editor (`regedit.exe`).
- 2 Navigate to `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client`

If this key does not already exist, create this key.

- 3 Delete the value **Enabled** if it exists.
- 4 Create or edit the **DWORD** value **DisabledByDefault** and set it to **0**.
- 5 Restart the VMware Horizon View Composer service.

TLSv1.0 connections from View Composer to vCenter are now enabled.

- 6 In the Windows Registry on the View Composer machine, navigate to `HKLM\SOFTWARE\VMware, Inc.\VMware View Composer`.
- 7 Create or edit the String value **EnableTLS1.0** and set it to **1**.
- 8 If the View Composer host is a 64-bit machine, navigate to `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware View Composer`.
- 9 Create or edit the String value **EnableTLS1.0** and set it to **1**.
- 10 Restart the VMware Horizon View Composer service.

TLSv1.0 connections from View Composer to ESXi hosts are now enabled.

Enable Digest Access Authentication for View Composer

Effective in Horizon 7 version 7.0.3, View Composer has the basic access authentication method for web security enabled by default. For enhanced security, you can enable the digest access authentication method for View Composer.

Prerequisites

- Verify that you have View Composer 7.0.3 or a later release installed.
- Verify that you can log in to the View Composer machine as an Administrator.
- Verify that you have Connection Server 7.0.3 or later installed.

Procedure

- 1 Navigate to the directory where View Composer is installed.
- 2 Edit the `SviWebservice.exe.config` file.
- 3 For the `SslPoxBinding` configuration option, set `authenticationScheme="Digest"`.
- 4 For the `SslBasicAuth` configuration option, set `clientCredentialType="Digest"`.
- 5 Save and close the `SviWebservice.exe.config` file.
- 6 Edit the `SviConfig.exe.config` file.
- 7 For the `SslSviBinding` configuration option, set `clientCredentialType="Digest"`.
- 8 Save and close the `SviConfig.exe.config` file.
- 9 Restart the View Composer service.
 - a Start the Windows Services tool by entering `services.msc` at the command prompt.
 - b From the list of services, right-click the service you want to restart. For example, right-click VMware Horizon Composer 7.0.3.
 - c Click **Restart**.

Manually Upgrading the View Composer Database

Rather than letting the View Composer installer upgrade the database when a schema update is required, you can manually upgrade the database. You can use the `SviConfig` utility when you must observe the upgrade process more closely or when upgrade tasks must be distributed to IT administrators with different responsibilities.

When you upgrade View Composer to a version with an updated database schema, an installer prompt asks if you want the wizard to upgrade the database. If you choose not to use the installer wizard, you must use the `SviConfig` utility to upgrade the database and migrate the existing data.

Using the `SviConfig` command-line utility has the following advantages:

- This utility returns result codes and creates a log of the database upgrade to simplify troubleshooting if the upgrade fails.
- You can separate the upgrade tasks. A vSphere or Horizon 7 administrator can run the View Composer installer to upgrade the software. A database administrator (DBA) can use `SviConfig` to upgrade the View Composer database.

- The software upgrade and the database upgrade can occur during different maintenance windows. For example, your site might run database-maintenance operations on weekends only, whereas software-maintenance tasks can occur during the week.

Run SviConfig to Manually Upgrade the Database

With the SviConfig command-line utility, you can upgrade the View Composer database separately from the View Composer software. This utility also creates a log file to simplify troubleshooting if the upgrade fails.

Important Only experienced View Composer administrators should use the SviConfig utility. This utility is intended to resolve issues relating to the View Composer service.

Prerequisites

- Back up the View Composer database. For instructions, see the documentation for your database server.
- Verify that you know the database source name (DSN) for the View Composer database.
- Verify that you know the user name and password for the database administrator account for this database.

Procedure

- 1 On the vCenter Server virtual or physical machine, open a Windows command prompt and navigate to the SviConfig executable file.

The file is located with the View Composer application. The default path is C:\Program Files (86)\VMware\VMware View Composer\sviconfig.exe.

- 2 Enter the command to stop VMware View Composer.

```
net stop svid
```

- 3 Run the SviConfig databaseupgrade command.

```
sviconfig -operation=databaseupgrade
          -DsnName=target_DSN
          -Username=database_administrator_username
```

For example:

```
sviconfig -operation=databaseupgrade -dsname=LinkedClone
          -username=Admin
```

- 4 When prompted, supply the password.

A successful operation displays output that shows the upgrade steps.

```
Establishing database connection.
Database connection established successfully.
Upgrading database.
Load data from SVI_VC_CONFIG_ENTRY table.
```

```
Update SVI_DEPLOYMENT_GROUP table.
Update SVI_REPLICA table.
Update SVI_SIM_CLONE table.
SviConfig finished successfully.
Database is upgraded successfully.
```

- 5 Enter the command to start the View Composer.

net start svid

A complete log of the upgrade process is created and placed in C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log.

What to do next

If the database upgrade fails, see [Troubleshooting a View Composer Database Upgrade Failure](#).

If the result code is any number other than 0, which means success, see [Result Codes for a Manual Database Schema Update](#).

Result Codes for a Manual Database Schema Update

When you manually upgrade the View Composer database, the `sviconfig databaseupgrade` command displays a result code.

[Table 5-1. Result Codes for the databaseupgrade Command](#) shows the `sviconfig databaseupgrade` result codes.

Table 5-1. Result Codes for the databaseupgrade Command

Code	Description
0	The operation ended successfully.
1	The supplied DSN could not be found.
2	Invalid database administrator credentials were provided.
3	The driver for the database is not supported.
4	An unexpected problem arose and the command failed to complete.
14	Another application is using the View Composer service. Shut down the service before executing the command.
15	A problem arose during the restore process. Details are provided in the onscreen log output.
17	Unable to upgrade the database data.
18	Unable to connect to the database server.

Troubleshooting a View Composer Database Upgrade Failure

When you upgrade the View Composer service with the View Composer installer or run the `SviConfig databaseupgrade` command, the operation might fail to upgrade the View Composer database.

Problem

The SviConfig databaseupgrade operation displays error code 17, or the View Composer installer displays a warning message.

```
Database upgrade completed with warnings
```

Cause

The database-upgrade software contacts vCenter Server to get additional data about desktops. The database upgrade might fail if the desktops are not available, the ESXi host is not running, or vCenter Server is not available.

Solution

- 1 See the View Composer SviConfig log file for more information.

The default location of this file is C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log. The upgrade script logs a message for each failure.

- 2 Examine the log records to identify the desktops that failed to upgrade.

Option	Action
The desktop exists but is unavailable.	Make the desktop available again. Depending on the cause of the failure, you might have to restart the ESXi host or vCenter Server, or take another action.
The desktop does not exist.	Ignore the log message. Note A deleted desktop might appear to exist in Horizon Administrator if an administrator deletes the desktop virtual machine directly in vSphere.

- 3 Run the SviConfig databaseupgrade command again.

Migrate View Composer to Another Machine

In some situations, you might need to migrate a VMware Horizon View Composer service to a new Windows Server virtual or physical machine. For example, you might migrate View Composer and vCenter Server to a new ESXi host or cluster to expand your Horizon 7 deployment. In addition, View Composer and vCenter Server do not have to be installed on the same Windows Server machine.

You can migrate View Composer from the vCenter Server machine to a standalone machine or from a standalone machine to the vCenter Server machine.

Important These topics pertain to migrating the latest version of View Composer to another machine. You must upgrade from the earlier version of View Composer before you perform these tasks.

If your current version of View Composer is installed on a machine that does not meet the system requirements for the new version of View Composer, you cannot use these procedures. After you migrate View Composer to a system with a Windows Server operating system that is supported for this release, you can perform an in-place upgrade to the latest version of View Composer.

- **Guidelines for Migrating View Composer**

The steps you take to migrate the VMware Horizon View Composer service depend on whether you intend to preserve existing linked-clone virtual machines.

- **Migrate View Composer with an Existing Database**

When you migrate View Composer to another physical or virtual machine, if you intend to preserve your current linked-clone virtual machines, the new VMware Horizon View Composer service must continue to use the existing View Composer database.

- **Migrate View Composer Without Linked-Clone Virtual Machines**

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate View Composer to a new physical or virtual machine without migrating the RSA keys to the new machine. The migrated VMware Horizon View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

- **Prepare a Microsoft .NET Framework for Migrating RSA Keys**

To use an existing View Composer database, you must migrate the RSA key container between machines. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.

- **Migrate the RSA Key Container to the New View Composer Service**

To use an existing View Composer database, you must migrate the RSA key container from the source physical or virtual machine on which the existing VMware Horizon View Composer service resides to the machine on which you want to install the new VMware Horizon View Composer service.

Guidelines for Migrating View Composer

The steps you take to migrate the VMware Horizon View Composer service depend on whether you intend to preserve existing linked-clone virtual machines.

To preserve the linked-clone virtual machines in your deployment, the VMware Horizon View Composer service that you install on the new virtual or physical machine must continue to use the existing View Composer database. The View Composer database contains data that is required to create, provision, maintain, and delete the linked clones.

When you migrate the VMware Horizon View Composer service, you can also migrate the View Composer database to a new machine.

Whether or not you migrate the View Composer database, the database must be configured on an available machine in the same domain as the new machine on which you install the VMware Horizon View Composer service, or on a trusted domain.

View Composer creates RSA key pairs to encrypt and decrypt authentication information stored in the View Composer database. To make this data source compatible with the new VMware Horizon View Composer service, you must migrate the RSA key container that was created by the original VMware Horizon View Composer service. You must import the RSA key container to the machine on which you install the new service.

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate the service without using the existing View Composer database. You do not have to migrate the RSA keys, whether or not you use the existing database.

Note Each instance of the VMware Horizon View Composer service must have its own View Composer database. Multiple VMware Horizon View Composer services cannot share a View Composer database.

Migrate View Composer with an Existing Database

When you migrate View Composer to another physical or virtual machine, if you intend to preserve your current linked-clone virtual machines, the new VMware Horizon View Composer service must continue to use the existing View Composer database.

Follow the steps in this procedure when you migrate View Composer in any of the following directions:

- From a vCenter Server machine to a standalone machine
- From a standalone machine to a vCenter Server machine
- From a standalone machine to another standalone machine
- From a vCenter Server machine to another vCenter Server machine

When you migrate the VMware Horizon View Composer service, you can also migrate the View Composer database to a new location. For example, you might need to migrate the View Composer database if the current database is located on a vCenter Server machine that you are migrating as well.

When you install the VMware Horizon View Composer service on the new machine, you must configure the service to connect to the View Composer database.

Prerequisites

- Familiarize yourself with the View Composer migration requirements. See [Guidelines for Migrating View Composer](#).
- Familiarize yourself with the steps for migrating the RSA key container to the new VMware Horizon View Composer service. See [Prepare a Microsoft .NET Framework for Migrating RSA Keys](#) and [Migrate the RSA Key Container to the New View Composer Service](#).

- Familiarize yourself with installing the VMware Horizon View Composer service in the *Horizon 7 Installation* document.
- Familiarize yourself with configuring an TLS certificate for View Composer in the *Horizon 7 Installation* document.
- Familiarize yourself with configuring View Composer in Horizon Administrator. See the topics about configuring View Composer settings and View Composer domains in the *Horizon 7 Administration* document.
- As best practice, verify that the source and destination machines that you use for migrating View Composer are identical and share the same administrator credentials. When you migrate View Composer from a standalone machine to a vCenter Server machine that already has View Composer installed, configuring View Composer might fail if the credentials used on the two machines are different.

Procedure

- 1 Disable virtual machine provisioning in the vCenter Server instance that is associated with the VMware Horizon View Composer service.
 - a In Horizon Administrator, select **View Configuration > Servers**.
 - b On the **vCenter Servers** tab, select the vCenter Server instance and click **Disable Provisioning**.
- 2 (Optional) Migrate the View Composer database to a new location.

If you need to take this step, consult your database administrator for migration instructions.
- 3 Uninstall the VMware Horizon View Composer service from the current machine.
- 4 (Optional) Migrate the RSA key container to the new machine.
- 5 Install the VMware Horizon View Composer service on the new machine.

During the installation, specify the DSN of the database that was used by the original VMware Horizon View Composer service. Also specify the domain administrator user name and password that were provided for the ODBC data source for that database.

If you migrated the database, the DSN and data source information must point to the new location of the database. Whether or not you migrated the database, the new VMware Horizon View Composer service must have access to the original database information about the linked clones.
- 6 Configure an SSL server certificate for View Composer on the new machine.

You might be able to copy the certificate that was installed for View Composer on the original machine, or you can install a new certificate.
- 7 In Horizon Administrator, configure the new View Composer settings.
 - a In Horizon Administrator, select **View Configuration > Servers**.
 - b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with this View Composer service and click **Edit**.

- c In the View Composer Server Settings pane, click **Edit** and provide the new View Composer settings.

If you are installing View Composer with vCenter Server on the new machine, select **View Composer co-installed with the vCenter Server**.

If you are installing View Composer on a standalone machine, select **Standalone View Composer Server** and provide the FQDN of the View Composer machine and the user name and password of the View Composer user.

- d In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.
- e Click **OK**.

Migrate View Composer Without Linked-Clone Virtual Machines

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate View Composer to a new physical or virtual machine without migrating the RSA keys to the new machine. The migrated VMware Horizon View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

Prerequisites

- Familiarize yourself with installing the VMware Horizon View Composer service in the *Horizon 7 Installation* document.
- Familiarize yourself with configuring a TLS certificate for View Composer in the *Horizon 7 Installation* document.
- Familiarize yourself with the steps for removing View Composer from Horizon Administrator. See topic about removing View Composer from Horizon Administrator in the *Horizon 7 Administration* document.

Before you can remove View Composer, verify that it no longer manages any linked-clone virtual machines. If any linked clones remain, you must delete them.

- Familiarize yourself with configuring View Composer in Horizon Administrator. See the topics about configuring View Composer settings and View Composer domains in the *Horizon 7 Administration* document.

Procedure

- 1 In Horizon Administrator, remove View Composer from Horizon Administrator.
 - a Select **View Configuration > Servers**.
 - b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with the View Composer service and click **Edit**.
 - c In the View Composer Server Settings pane, click **Edit**.
 - d Select **Do not use View Composer** and click **OK**.

- 2 Uninstall the VMware Horizon View Composer service from the current machine.

- 3 Install the VMware Horizon View Composer service on the new machine.

During the installation, configure View Composer to connect to the DSN of the original or new View Composer database.

- 4 Configure a TLS server certificate for View Composer on the new machine.

You might be able to copy the certificate that was installed for View Composer on the original machine, or you can install a new certificate.

- 5 In Horizon Administrator, configure the new View Composer settings.

- a In Horizon Administrator, select **View Configuration > Servers**.
- b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with this View Composer service and click **Edit**.
- c In the View Composer Server Settings pane, click **Edit**.
- d Provide the new View Composer settings.

If you are installing View Composer with vCenter Server on the new machine, select **View Composer co-installed with the vCenter Server**.

If you are installing View Composer on a standalone machine, select **Standalone View Composer Server** and provide the FQDN of the View Composer machine and the user name and password of the View Composer user.

- e In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.
- f Click **OK**.

Prepare a Microsoft .NET Framework for Migrating RSA Keys

To use an existing View Composer database, you must migrate the RSA key container between machines. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.

Prerequisites

Download the .NET Framework and read about the ASP.NET IIS registration tool. Go to <http://www.microsoft.com/net>.

Procedure

- 1 Install the .NET Framework on the physical or virtual machine on which the VMware Horizon View Composer service associated with the existing database is installed.
- 2 Install the .NET Framework on the destination machine on which you want to install the new VMware Horizon View Composer service.

What to do next

Migrate the RSA key container to the destination machine. See [Migrate the RSA Key Container to the New View Composer Service](#).

Migrate the RSA Key Container to the New View Composer Service

To use an existing View Composer database, you must migrate the RSA key container from the source physical or virtual machine on which the existing VMware Horizon View Composer service resides to the machine on which you want to install the new VMware Horizon View Composer service.

You must perform this procedure before you install the new VMware Horizon View Composer service.

Prerequisites

Verify that the Microsoft .NET Framework and the ASP.NET IIS registration tool are installed on the source and destination machines. See [Prepare a Microsoft .NET Framework for Migrating RSA Keys](#).

Procedure

- 1 On the source machine on which the existing VMware Horizon View Composer service resides, open a command prompt and navigate to the %windir%\Microsoft.NET\Framework\v2.0.xxxx directory.

- 2 Type the `aspnet_regiis` command to save the RSA key pair in a local file.

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

The ASP.NET IIS registration tool exports the RSA public-private key pair from the SviKeyContainer container to the `keys.xml` file and saves the file locally.

- 3 Copy the `keys.xml` file to the destination machine on which you want to install the new VMware Horizon View Composer service.
- 4 On the destination machine, open a command prompt and navigate to the %windir%\Microsoft.NET\Framework\v2.0.xxxx directory.
- 5 Type the `aspnet_regiis` command to migrate the RSA key pair data.

```
aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp
```

where *path* is the path to the exported file.

The `-exp` option creates an exportable key pair. If a future migration is required, the keys can be exported from this machine and imported to another machine. If you previously migrated the keys to this machine without using the `-exp` option, you can import the keys again using the `-exp` option so that you can export the keys in the future.

The registration tool imports the key pair data into the local key container.

What to do next

Install the new VMware Horizon View Composer service on the destination machine. Provide the DSN and ODBC data source information that allows View Composer to connect to the same database information that was used by the original VMware Horizon View Composer service. For installation instructions, see "Installing View Composer" in the *Horizon 7 Installation* document.

Complete the steps to migrate View Composer to a new machine and use the same database. See [Migrate View Composer with an Existing Database](#).

Upgrading Horizon Connection Server

If your deployment uses load balancers to manage multiple Connection Server instances, an upgrade of the Connection Server infrastructure can be performed with zero down time.

Note Before you can use the Horizon 6 version 6.2 feature for cloning a desktop pool, you must upgrade all Connection Server instances in a pod to Horizon 6 version 6.2 or later.

After you have performed a fresh install or upgraded all Connection Server instances to Horizon 7 version 7.2, you cannot downgrade the Connection Server instances to a version earlier than Horizon 7 version 7.2 because the keys used to protect LDAP data have changed.

To keep the possibility of downgrading Connection Server instances while planning an upgrade to Horizon 7 version 7.2, you must backup the Connection Server instances before starting the upgrade. If you need to downgrade the Connection Server instances, you must downgrade all Connection Server instances and then apply the backup to the last Connection Server that is downgraded.

When upgrading from a version of Horizon 7 earlier than Horizon 7 version 7.8, some user authentication settings will change. How these user authentication settings affect the user experience depends upon the client. See the Horizon Client documentation at <https://docs.vmware.com/en/VMware-Horizon-Client/index.html>. You must understand the usability and security implications of the user authentication settings before changing them. See, "Security-Related Server Settings for User Authentication" in the *Horizon 7 Security* document.

Preparing Connection Server for an Upgrade

Before you upgrade Connection Server or before you upgrade any of the vSphere components that Connection Server relies on, you must perform several tasks to ensure that these upgrades are successful.

Tasks to Perform on Only One Instance in a Replicated Group

Before you begin upgrading any Connection Server instances, perform the following tasks using only one of the instances. Because the instances are replicated, the settings on one instance are the same as the settings on the others:

- If Connection Server is installed in a virtual machine, take a snapshot of the virtual machine.

For instructions on taking snapshots, see the vSphere Client online help. If you ever need to revert to this snapshot and if you have other Connection Server instances in a replicated group, you must uninstall those instances before you revert the master to the snapshot. After you revert, you can reinstall the replicated instances and point to the instance you reverted.

You can label the snapshot Upgrade Preparation Phase.

- Open Horizon Administrator and document all the global settings and settings for desktops and pools: Pools section and Desktops section in the Inventory tree, and the Global Settings section in the View Configuration tree.

For example, take a screen shot of the applicable settings.

- Use the `vdmexport.exe` utility to back up the LDAP database.

For instructions, see the administration guide for your current version of the *Horizon 7 Administration* document.

Tasks to Perform for Each Instance Just Before Upgrading

- Verify that the virtual or physical machine on which the current Connection Server instance is installed meets the system requirements for the new version.

See [Horizon Connection Server Requirements](#).

- Document the IP address and system name of the machine on which Connection Server is installed.
- Determine if your company has written any batch files or scripts that run against the View database on the Connection Server instance, and if so, document their names and locations.
- Open Horizon Administrator and document all the settings that are specific to this instance.

For example, go to **View Configuration > Servers > Connection Servers**, select the Connection Server instance in the table and click **Edit**. You can take a screen shot of each tab in the **Edit Connection Server Settings** dialog box.

Upgrade Connection Servers in a Replicated Group

This procedure describes upgrading Connection Server instances that are not paired with security servers. For example, this procedure applies to Connection Servers that are configured for connections to clients that are inside the corporate firewall.

For Connection Server instances that are paired with security servers, use the procedure described in [Upgrade Security Servers and Their Paired Connection Servers](#).

You do not need to reboot the Connection Server after the upgrade completes.

Note This procedure describes an in-place upgrade. To migrate to a different machine, see [Upgrade to the Latest Version of Connection Server on a Different Machine](#).

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. The amount of time the upgrade takes depends on the number of Connection Server instances in the group. Budget 15 minutes to half an hour for each instance.
- If you use View Composer, verify that View Composer has been upgraded. See [Upgrade View Composer](#). After you upgrade Connection Server, you must add View Composer using Horizon Administrator.
- Familiarize yourself with the security-related requirements of Horizon 7, and verify that these requirements are met. See [Upgrade Requirements for Horizon Connection Server](#). You might need to obtain and install a CA-signed SSL server certificate that includes certificate revocation information, verify that Windows Firewall with Advanced Security is set to **on**, and configure any back-end firewalls to support IPsec.
- Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in Horizon Administrator, and a message indicates that vCenter Server is unavailable.
- Complete the tasks listed in [Preparing Connection Server for an Upgrade](#).
- Verify that you have a license that is valid for the new version.

Note When you upgrade from 6.0.x or 6.1.x to 6.2, your previous license will continue to work and the usage model will be set to **Concurrent User**. A new licensing model called Named User was added beginning with Horizon 6 version 6.2. You have the option of changing the licensing model to **Named User**. For more information, see <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- If you are unfamiliar with the `vdmexport.exe` utility, print the instructions for using it from the *Horizon 7 Administration* document. You will use this utility to back up the View LDAP database as part of the upgrade procedure.

You do not need to make any changes to the configuration of existing load balancers.

Procedure

- 1 If you are using a load balancer to manage a group of Connection Server instances, disable the server that hosts the Connection Server instance that you are about to upgrade.
 - a Log in to Horizon Administrator.
 - b Go to **View Configuration > Servers** and click the **Connection Servers** tab.
 - c Select the Connection Server instance in the list and click the **Disable** button above the table.
 - d Click **OK** to confirm disabling the server.

- 2 On the host of the Connection Server instance, download and run the installer for the new version of Connection Server.

The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where `xxxxxx` is the build number and `y.y.y` is the version number. You do not need to stop any services before performing the upgrade. The installer stops and restarts services as necessary. In fact, the `VMwareVDMDS` service must be running in order to upgrade the View LDAP database.

The installer determines that an older version is already installed and performs an upgrade. The installer displays fewer installation options than during a fresh installation.

The View LDAP is also upgraded.

Note Before performing the upgrade, the installer does a replication status check to determine whether the server can communicate with the other servers in the replicated group and whether the server can fetch LDAP updates from the other servers in the group. If the status check fails, the upgrade does not proceed.

- 3 Verify that the VMware Horizon Connection Server service restarts after the installer wizard closes.
- 4 Log in to Horizon Administrator and enable the Connection Server instance that you just upgraded.
 - a Go to **View Configuration > Servers** and click the **Connection Servers** tab.
 - b Select the Connection Server instance in the list and click the **Enable** button above the table.
 - c In the Version column, verify that the new version is displayed.
- 5 Go to **View Configuration > Product Licensing and Usage**, click **Edit License**, enter the license key, and click **OK**.
- 6 If you are using a load balancer for managing this Connection Server instance, enable the server that you just upgraded.
- 7 Verify that you can log in to a remote desktop.
- 8 Repeat the previous steps to upgrade each Connection Server instance in the group.

Important If you do not upgrade all Connection Server instances in a replicated group, the health indicators in the Horizon Administrator dashboard might show that one or more instances are in an error state. This situation arises because different versions supply different kinds of data. The solution is to upgrade all instances in the replicated group.

- 9 Use the `vdmexport.exe` utility to back up the newly upgraded View LDAP database.

If you have multiple instances of Connection Server in a replicated group, you need only export the data from one instance.
- 10 Log in to Horizon Administrator and examine the dashboard to verify that the vCenter Server and View Composer icons are green.

If either of these icons is red and an Invalid Certificate Detected dialog box appears, you must click **Verify** and either accept the thumbprint of the untrusted certificate, as described in "What to Do Next," or install a valid CA-signed SSL certificate.

For information about replacing the default certificate for vCenter Server, see the *VMware vSphere Examples and Scenarios* document.

11 Verify that the dashboard icons for the connection server instances are also are green.

If any instances have red icons, click the instance to determine the replication status. Replication might be impaired for any of the following reasons:

- A firewall might be blocking communication
- The VMware VDMDS service might be stopped on a Connection Server instance
- The VMware VDMS DSA options might be blocking the replications
- A network problem has occurred

What to do next

To use a default or self-signed certificate from vCenter Server or View Composer, see [Accept the Thumbprint of a Default TLS Certificate](#).

If you have an older version of vCenter Server, see [Enable TLSv1.0 on vCenter Connections from Connection Server](#).

If the upgrade fails on one or more of the Connection Server instances, see [Create a Replicated Group After Reverting Connection Server to a Snapshot](#).

Important If you plan to use enhanced message security mode for JMS messages, make sure that firewalls allow Connection Server instances to receive incoming JMS traffic on port 4002 from desktops and security servers. Also open port 4101 to accept connections from other Connection Server instances.

If you ever reinstall Connection Server on a server that has a data collector set configured to monitor performance data, stop the data collector set and start it again.

Enable TLSv1.0 on vCenter Connections from Connection Server

Horizon 7 and later components have the TLSv1.0 security protocol disabled by default. If your deployment includes an older version of vCenter Server that supports only TLSv1.0, you might need to enable TLSv1.0 for Connection Server connections after installing or upgrading to Connection Server 7.0 or a later release.

Some earlier maintenance releases of vCenter Server 5.1, and 5.5 support only TLSv1.0, which is no longer enabled by default in Horizon 7 and later releases. If it is not possible to upgrade vCenter Server to a version that supports TLSv1.1 or TLSv1.2, you can enable TLSv1.0 for Connection Server connections.

Prerequisites

- If you are upgrading to Horizon 7, perform this procedure before you upgrade to minimize the number of times you must restart the service. During an upgrade the Connection Server service is restarted, and a restart is required to apply the configuration changes described in this procedure. If you upgrade before you perform this procedure, you will need to restart the service a second time.

- See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.

Procedure

- 1 Start the ADSI Edit utility on your Connection Server host.
- 2 In the console tree, select **Connect to**.
- 3 In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name **DC=vdi, DC=vmware, DC=int**.
- 4 In the Computer pane, select or type **localhost:389** or the fully qualified domain name (FQDN) of the Connection Server host followed by port 389.

For example: **localhost:389** or **mycomputer.example.com:389**

- 5 Expand the ADSI Edit tree, expand **OU=Properties**, select **OU=Global**, and double-click **CN=Common** in the right pane.
- 6 In the Properties dialog box, edit the **pae-ClientSSLSecureProtocols** attribute to add the following value

\LIST:TLSv1.2,TLSv1.1,TLSv1

Be sure to include the back slash at the beginning of the line.

- 7 Click **OK**.
- 8 If this is a fresh installation, to apply the configuration change, restart the Connection Server service on each connection server instance.

If you plan to perform an upgrade, you do not need to restart the service because the process of upgrading automatically restarts the service.

Upgrade to the Latest Version of Connection Server on a Different Machine

As part of your upgrade, you can migrate Connection Server to a new machine.

Prerequisites

- Upgrade at least one existing Connection Server instance to the latest version. See [Upgrade Connection Servers in a Replicated Group](#). During this upgrade, your existing View LDAP will be upgraded.
- Verify that the new physical or virtual machine meets the system requirements for installing Connection Server. See [Supported Operating Systems for Horizon Connection Server](#) and [Hardware Requirements for Horizon Connection Server](#).
- Familiarize yourself with the security-related requirements of Horizon 7, and verify that these requirements are met. See [Upgrade Requirements for Horizon Connection Server](#).
- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.

- Verify that you have a domain user account with administrative privileges on the host you will use to run the installer.
- Familiarize yourself with the procedure for installing a replicated instance. See the *Horizon 7 Installation* document. You install a replicated instance as part of this procedure.

You do not need to make any changes to the configuration of existing load balancers.

Procedure

- 1 Verify that an upgraded instance of Connection Server is running and is accessible to the new machine where you plan to install Connection Server.

When you install Connection Server on the new host, you will point to this existing instance.

- 2 On the new machine, install a replicated instance of Connection Server.

The View LDAP on the new instance will replicate that of the upgraded source instance.

- 3 If applicable, uninstall Connection Server from the old host by using the Windows **Add/Remove Programs** utility.

- 4 In Horizon Administrator, go to **View Configuration > Servers > Connection Servers** tab and determine whether the Connection Server instance that was uninstalled still appears in the list.

- 5 If the uninstalled Connection Server instance still appears in the list, use a `vdadmin` command to remove it.

```
vdadmin.exe -S -s server_name -r
```

In this example, `server_name` is the host name or IP address of the Connection Server host. For more information about the `vdadmin` command-line tool, see the *Horizon 7 Administration* document.

A new instance of Connection Server is added to a group and an old instance is removed.

What to do next

If you have an older version of vCenter Server, see [Enable TLSv1.0 on vCenter Connections from Connection Server](#).

Upgrade the other Horizon 7 server components.

If you ever reinstall Connection Server on a server that has a data collector set configured to monitor performance data, stop the data collector set and start it again.

Create a Replicated Group After Reverting Connection Server to a Snapshot

If an upgrade fails, or if for some other reason, you must revert a virtual machine that hosts Connection Server to a snapshot, you must uninstall the other Connection Server instances in the group and recreate the replicated group.

If you revert one Connection Server virtual machine to a snapshot, the View LDAP objects in the database of that virtual machine are no longer consistent with the View LDAP objects in the databases of the other replicated instances. After you revert to a snapshot, the following event is logged in the Windows Event log, in the VMwareVDMDS Event log (Event ID 2103): The Active Directory Lightweight Directory Services database has been restored using an unsupported restoration procedure. The reverted virtual machine stops replicating its View LDAP.

If you find it necessary to revert to a snapshot, you must uninstall other Connection Server instances and uninstall the View LDAP on those virtual machines and then reinstall replica instances.

Prerequisites

Determine which Connection Server instance is to be the new standard, or master, Connection Server. This Connection Server has the desired Horizon 7 configuration data.

Procedure

- 1 On all Connection Server instances except the one chosen to be the new standard Connection Server instance, uninstall Connection Server and the View LDAP instance.

The View LDAP instance is called AD LDS Instance VMwareVDMDS.

- 2 On the virtual machine that hosts the standard, or master, Connection Server instance, open a command prompt and enter the following command to ensure that replication is not disabled.

```
repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL -DISABLE_INBOUND_REPL
```

- 3 On the virtual machines that are to host the replica Connection Server instances, run the Connection Server installer, select the **View Replica Server** installation option, and specify the host name or IP address of the standard Connection Server instance.

The replicated group of Connection Server instances is recreated and their View LDAP objects are consistent.

Upgrading Security Servers

If your deployment uses load balancers to manage multiple security servers, you can perform an upgrade of the Connection Server infrastructure with zero down time.

Note To use Unified Access Gateway appliances instead of security servers, you must upgrade the Connection Server instances to Horizon 6 version 6.2 or later before installing and configuring the Unified Access Gateway appliances to point to the Connection Server instances, or the load balancer that fronts the instances. For more information, see [Replacing a Security Server with a Unified Access Gateway Appliance](#).

Preparing Security Server for an Upgrade

Before you upgrade security servers, perform these tasks to create backups and record configuration settings.

- Verify that the virtual or physical machine on which the current security server is installed meets the system requirements for the new version.

See [Horizon Connection Server Requirements](#).
- If the security server is installed in a virtual machine, take a snapshot of the virtual machine.

For instructions on taking snapshots, see the vSphere Client online help. You can label the snapshot Upgrade Preparation Phase.
- Open Horizon Administrator and document the settings for this security server. Go to **View Configuration > Servers** and click the **Security Servers** tab.

For example, select the security server, click **Edit**, and take a screen shot of the settings.
- Document the IP address and system name of the machine on which the security server is installed.
- If you use load balancers for security servers, document the configuration settings for the load balancers.

Note This topic does not describe the Horizon Administrator command called **Prepare for Upgrade or Reinstallation**, which is available from the **Security Servers** tab. That command removes IPsec rules for the security server, which stops all communication between the security server and the paired Connection Server instance. You will therefore use the command during the upgrade procedure, immediately before you upgrade the security server, as described in [Upgrade Security Servers and Their Paired Connection Servers](#).

Upgrade Security Servers and Their Paired Connection Servers

Use this procedure if the Connection Server instance that you plan to upgrade is paired with a security server.

This procedure is designed to upgrade one security server and its paired Connection Server instance before moving on to upgrade the next security server and its paired Connection Server instance. This strategy allows for zero down time. If the instance is not paired with a security server, use the procedure [Upgrade Connection Servers in a Replicated Group](#).

The first few steps of this procedure involve upgrading the Connection Server instance. After the Connection Server upgrade, but before the security server upgrade, one of the steps describes removing the IPsec rules for the security server. When you remove the IPsec rules for an active security server, all communication with the security server is lost until you upgrade or reinstall the security server.

By default, communication between a security server and its paired Connection Server instance is governed by IPsec rules. If the existing IPsec rules are not removed before you upgrade or reinstall, the pairing between the security server and Connection Server fails, and a new set of IPsec rules cannot be established after the upgrade.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 to 30 minutes for each security server and its paired Connection Server instance.
- If you use View Composer, verify that View Composer has been upgraded. See [Upgrade View Composer](#). After you upgrade Connection Server, you must add View Composer using Horizon Administrator.
- Familiarize yourself with the security-related requirements of Horizon 7, and verify that these requirements are met. See [Upgrade Requirements for Horizon Connection Server](#). You might need to obtain and install a CA-signed TLS server certificate that includes certificate revocation information, verify that Windows Firewall with Advanced Security is set to **on**, and configure any back-end firewalls to support IPsec.
- Verify that the virtual or physical machines on which the current security server and Connection Server instances are installed meet the system requirements.
See [Horizon Connection Server Requirements](#).
- Complete the tasks listed in [Preparing Connection Server for an Upgrade](#).
- Verify that you have a license for the new version.
- Verify that you have a user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- Verify that the Connection Server instance to be paired with the security server is accessible to the computer on which you plan to install the security server.

Note After a Connection Server upgrade to Horizon 7 version 7.5, security servers with IPsec disabled must be reinstalled. If the IP address of a security server changes it must be reinstalled. Security server pairing does not work correctly if the security server is behind Dynamic NAT.

Procedure

- 1 If you are using a load balancer to manage security servers that are paired with Connection Server instances, disable the security server that is paired with the Connection Server instance you are about to upgrade.
- 2 Upgrade the Connection Server instance that is paired with this security server.
Follow steps 2 through 6 of [Upgrade Connection Servers in a Replicated Group](#).

- 3 Remove IPsec rules for the security server paired with the Connection Server instance that you just upgraded.

- a In Horizon Administrator, click **View Configuration > Servers**.
- b In the **Security Servers** tab, select a security server and click **More Commands > Prepare for Upgrade or Reinstallation**.

If you disabled IPsec rules before you installed the security server, this setting is inactive. In this case, you do not have to remove IPsec rules before you reinstall or upgrade.

- c Click **OK**.

The IPsec rules are removed and the **Prepare for Upgrade or Reinstallation** setting becomes inactive, indicating that you can reinstall or upgrade the security server.

- 4 Configure a security server pairing password using the latest version of Horizon Administrator. See, "Configure a Security Server Pairing Password" in the *Horizon 7 Installation* document.
- 5 On the host of the security server, download and run the installer for the latest version of Connection Server.

The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where `xxxxxx` is the build number and `y.y.y` is the version number. The installer determines that an older version is already installed and performs an upgrade. The installer displays fewer installation options than during a fresh installation.

You will be prompted to supply the security server pairing password.

You might be prompted to dismiss a message box notifying you that the Security Server service was stopped. The installer stops the service in preparation for the upgrade.

- 6 After the installer wizard is finished, verify that the VMware Horizon View Security Server service is started.
- 7 If you are using a load balancer for managing this security server, add this server back to the load-balanced group.
- 8 Log in to Horizon Administrator, select the security server in the Dashboard, and verify that the security server is now at the latest version.
- 9 Verify that you can log in to a remote desktop.
- 10 In Horizon Administrator, go to **View Configuration > Servers > Security Servers** tab and remove any duplicate security servers from the list.

The automated security server pairing mechanism can produce duplicate entries in the **Security Servers** list if the full system name does not match the name that was assigned when the security server was originally created.

- 11 Use the `vdmexport.exe` utility to back up the newly upgraded View LDAP database.

If you have multiple instances of Connection Server in a replicated group, you need only export the data from one instance.

- 12 Log in to Horizon Administrator and examine the dashboard to verify that the vCenter Server and View Composer icons are green.

If either of these icons is red and an Invalid Certificate Detected dialog box appears, you must click **Verify** and either accept the thumbprint of the untrusted certificate, as described in "What to Do Next," or install a valid CA-signed SSL certificate.

For information about replacing the default certificate for vCenter Server, see the *VMware vSphere Examples and Scenarios* document.

- 13 Verify that the dashboard icons for the connection server instances are also are green.

If any instances have red icons, click the instance to determine the replication status. Replication might be impaired for any of the following reasons:

- A firewall might be blocking communication
- The VMware VDMDS service might be stopped on a Connection Server instance
- The VMware VDMS DSA options might be blocking the replications
- A network problem has occurred

What to do next

To use a default or self-signed certificate from vCenter Server or View Composer, see [Accept the Thumbprint of a Default TLS Certificate](#).

If the upgrade fails on one or more of the Connection Server instances, see [Create a Replicated Group After Reverting Connection Server to a Snapshot](#).

Important If you plan to use enhanced message security mode for JMS messages, make sure that firewalls allow Connection Server instances to receive incoming JMS traffic on port 4002 from desktops and security servers. Also open port 4101 to accept connections from other Connection Server instances.

If you ever reinstall Connection Server on a server that has a data collector set configured to monitor performance data, stop the data collector set and start it again.

Replacing a Security Server with a Unified Access Gateway Appliance

You can replace a security server with a Unified Access Gateway appliance.

Prerequisites

To use Unified Access Gateway appliances instead of security servers, you must upgrade the Connection Server instances to Horizon 6 version 6.2 or later before installing and configuring the Unified Access Gateway appliances to point to the Connection Server instances, or the load balancer that fronts the instances.

Procedure

- 1 Uninstall the security server software.

- 2 Remove the IPsec configuration for the security server. See *Remove IPsec Rules for the Security Server* in the *Horizon 7 Installation* document.
- 3 Remove the security server's LDAP entry. See *Removing the Entry for a Connection Server Instance or Security Server Using the -S Option* in the *Horizon 7 Administration* document.
- 4 In Horizon Administrator, register the Unified Access Gateway appliance.
- 5 At the network firewall between Unified Access Gateway and Connection Server, remove firewall rules associated with the removed security server and add firewall rules associated with the incoming Unified Access Gateway. The Unified Access Gateway needs to communicate with Connection Server on TCP port 443.

The back-end firewall rules for Security Server to Connection Server are as follows:

Source	Default Port	Protocol	Destination	Default Port	Notes
Security Server	UDP 500	ISAKMP	Connection Server	UDP 500	IPsec phase 1 negotiation.
Security Server	UDP 4500	NAT-T	Connection Server	UDP 4500	Encapsulated AJP13 traffic when using NAT.
Security Server		ESP	Connection Server		Encapsulated AJP13 traffic when NAT traversal is not required. ESP is IP protocol 50. Port numbers are not specified.
Security Server		AJP13	Connection Server	TCP 8009	AJP13 traffic without IPsec and during pairing.
Security Server		JMS	Connection Server	TCP 4001	Message channel for key negotiation.
Security Server		JMS-TLS	Connection Server	TCP 4002	Message channel for management.

- 6 Configure and start the Unified Access Gateway appliance.

See *Deploying and Configuring VMware Unified Access Gateway* document in <https://docs.vmware.com/en/Unified-Access-Gateway/index.html>.

Upgrading a Cloud Pod Architecture Environment

The Cloud Pod Architecture feature uses standard Horizon 7 components to provide cross-data center administration. With the Cloud Pod Architecture feature, you link together multiple pods to provide a single large desktop and application brokering and management environment. A pod consists of a set of Connection Server instances, shared storage, a database server, and the vSphere and network infrastructures required to host desktop and application pools.

Use the following process to upgrade a Cloud Pod Architecture environment.

- 1 Upgrade all Connection Server instances in one pod, according to the usual process for upgrading a single Connection Server instance.
- 2 Repeat the preceding step for the other pods in the pod federation, upgrading each pod one-by-one.

During the upgrade process, some Connection Server instances use the latest version of Horizon 7 and some use the older version. Although this mixed-version environment is supported beginning with Horizon 7 version 7.4, new features do not work in a mixed environment. For example, a new feature that is visible in Horizon Administrator on an upgraded server is not visible in Horizon Administrator on a server that has not been upgraded.

For information about designing and setting up a Cloud Pod Architecture environment, see *Administering Cloud Pod Architecture in Horizon 7*.

Upgrading Horizon 7 Servers to Allow HTML Access

When upgrading Connection Server instances or security servers behind a load balancer or behind a gateway such as Unified Access Gateway, you must make configuration changes to continue to use HTML Access.

For more information, see "Allow HTML Access Through a Load Balancer" and "Allow HTML Access Through a Gateway" in the *Horizon 7 Installation* document.

Upgrade vCenter Server

Perform a vCenter Server upgrade as part of the same maintenance window during which you upgrade other Horizon 7 server components. Before you upgrade vCenter Server, you must back up some Horizon 7 data. After the upgrade, if View Composer is running on the same server, you must restart the View Composer service.

Note During the vCenter Server upgrade, existing remote desktop and application sessions will not be disconnected, but the following functionality is not available during the vCenter Server upgrade:

- Remote desktops that are in a provisioning state will not get powered on.
 - New desktops cannot be launched.
 - View Composer operations are not allowed.
-

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. For information about how much time is required, see the *VMware vSphere Upgrade Guide*.
- Back up the vCenter Server database and the View Composer database.
- Back up the View LDAP database from a Connection Server instance by using the `vdmexport.exe` utility.

For instructions, see the *Horizon 7 Administration* document. If you have multiple instances of Connection Server in a replicated group, you need to export the data from only one instance.

- Perform the tasks listed in [Preparing for Upgrades That Include vSphere](#).

- Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed TLS server certificate installed and configured. After you upgrade Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in Horizon Administrator, and a message indicates that vCenter Server is unavailable.
- Complete the prerequisites listed in the *VMware vSphere Upgrade Guide*, using the version of the guide that corresponds to the version of vSphere that you plan to upgrade to.
- To upgrade vCenter Server while instant clones are in use, see the steps in the VMware Knowledge Base (KB) article <https://kb.vmware.com/s/article/52573>.

Procedure

- 1 Upgrade vCenter Server as described in the *VMware vSphere Upgrade Guide*.

Important If your clusters contain vSAN datastores, also see the chapter about upgrading the vSAN cluster, in the *Administering VMware vSAN* document. This chapter contains a topic about upgrading vCenter Server.

- 2 If View Composer is installed on the same host, restart the View Composer service.
- 3 Log in to Horizon Administrator and examine the dashboard to verify that the vCenter Server and View Composer icons are green.

If either of these icons is red and an Invalid Certificate Detected dialog box appears, you must click **Verify** and either accept the thumbprint of the untrusted certificate, as described in "What to Do Next," or install a valid CA-signed SSL certificate.

For information about replacing the default certificate for vCenter Server, see the *VMware vSphere Examples and Scenarios* document.

What to do next

To use a default or self-signed certificate from vCenter Server or View Composer, see [Accept the Thumbprint of a Default TLS Certificate](#).

If you have finished upgrading Horizon 7 server components, at your next maintenance window, continue with the Horizon 7 upgrade.

- If you are also upgrading vSphere components, see [Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines](#).
- If you upgrading only Horizon 7 components, see [Upgrade View Agent or Horizon Agent](#).

Accept the Thumbprint of a Default TLS Certificate

When you add vCenter Server and View Composer instances to Horizon 7, you must ensure that the TLS certificates that are used for the vCenter Server and View Composer instances are valid and trusted by Connection Server. If the default certificates that are installed with vCenter Server and View Composer are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server or View Composer instance is configured with a certificate that is signed by a CA, and the root certificate is trusted by Connection Server, you do not have to accept the certificate thumbprint. No action is required.

If you replace a default certificate with a certificate that is signed by a CA, but Connection Server does not trust the root certificate, you must determine whether to accept the certificate thumbprint. A thumbprint is a cryptographic hash of a certificate. The thumbprint is used to quickly determine if a presented certificate is the same as another certificate, such as the certificate that was accepted previously.

Note If you install vCenter Server and View Composer on the same Windows Server host, they can use the same TLS certificate, but you must configure the certificate separately for each component.

For details about configuring TLS certificates, see "Configuring TLS Certificates for View Servers" in the *Horizon 7 Installation* document.

You first add vCenter Server and View Composer in Horizon Administrator by using the Add vCenter Server wizard. If a certificate is untrusted and you do not accept the thumbprint, you cannot add vCenter Server and View Composer.

After these servers are added, you can reconfigure them in the Edit vCenter Server dialog box.

Note You also must accept a certificate thumbprint when you upgrade from an earlier release and a vCenter Server or View Composer certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

On the Horizon Administrator dashboard, the vCenter Server or View Composer icon turns red and an Invalid Certificate Detected dialog box appears. In Horizon Administrator, click **View Configuration > Servers** and edit the vCenter Server entry associated with the View Composer Service. Then, click **Edit** in the vCenter Server settings and follow the prompts to verify the and accept the self-signed certificate.

Similarly, in Horizon Administrator you can configure a SAML authenticator for use by a Connection Server instance. If the SAML server certificate is not trusted by Connection Server, you must determine whether to accept the certificate thumbprint. If you do not accept the thumbprint, you cannot configure the SAML authenticator in Horizon 7. After a SAML authenticator is configured, you can reconfigure it in the Edit Connection Server dialog box.

Procedure

- 1 When Horizon Administrator displays an Invalid Certificate Detected dialog box, click **View Certificate**.
- 2 Examine the certificate thumbprint in the Certificate Information window.

- 3 Examine the certificate thumbprint that was configured for the vCenter Server or View Composer instance.

- a On the vCenter Server or View Composer host, start the MMC snap-in and open the Windows Certificate Store.
- b Navigate to the vCenter Server or View Composer certificate.
- c Click the Certificate Details tab to display the certificate thumbprint.

Similarly, examine the certificate thumbprint for a SAML authenticator. If appropriate, take the preceding steps on the SAML authenticator host.

- 4 Verify that the thumbprint in the Certificate Information window matches the thumbprint for the vCenter Server or View Composer instance.

Similarly, verify that the thumbprints match for a SAML authenticator.

- 5 Determine whether to accept the certificate thumbprint.

Option	Description
The thumbprints match.	Click Accept to use the default certificate.
The thumbprints do not match.	Click Reject . Troubleshoot the mismatched certificates. For example, you might have provided an incorrect IP address for vCenter Server or View Composer.

Using Horizon 7 Group Policy Administrative Template Files

Horizon 7 provides several component-specific Group Policy Administrative ADMX template files. You can optimize and secure remote desktops and applications by adding the policy settings in the ADMX template files to a new or existing GPO in Active Directory.

All ADMX files that provide group policy settings for Horizon 7 are available in VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip, where x.x.x is the version and yyyyyy is the build number. You can download the file from the VMware Downloads site at <https://my.vmware.com/web/vmware/downloads>. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the ZIP file.

To upgrade group policies, use the Group Policy Object Editor on your Active Directory server to add the new version of the template files.

The Horizon 7 ADMX template files contain both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to all remote desktops, regardless of who connects to the desktop.
- The User Configuration policies set policies that apply to all users, regardless of the remote desktop or application they connect to. User Configuration policies override equivalent Computer Configuration policies.

Microsoft Windows applies policies at desktop startup and when users log in.

Upgrade ESXi Hosts and Their Virtual Machines

6

Upgrading ESXi hosts and virtual machines is the most time-consuming aspect of this middle phase of a Horizon 7 upgrade.

This procedure provides an overview of the tasks you must perform during the second and subsequent maintenance windows. To complete some of these tasks, you might need step-by-step instructions found in the *VMware vSphere Upgrade Guide* and the *Horizon 7 Administration* document.

For details about which versions of Horizon are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Important The following table describes which Horizon 7 features depend on specific virtual hardware versions and therefore might require a virtual machine upgrade.

Table 6-1. Virtual Hardware Versions Required for Specific Features

Feature	Virtual Hardware Version	Corresponding vSphere Version
Space-efficient disk format for linked-clone pools	9 or later	vSphere 5.1 or later
VMware [®] vSAN [®] datastores, first version	10 or later	vSphere 5.5 Update 1 or later
VMware vSAN datastores, second version	11 or later	vSphere 6.0 or later
VMware Virtual Volumes datastores	11 or later	vSphere 6.0 or later
Native NFS snapshot technology (VAAI)	9 or later	vSphere 5.1 or later
Virtual shared graphics acceleration	8 or later	vSphere 5.0 or later
Virtual dedicated graphics acceleration	9 or later	vSphere 5.1 or later
NVIDIA GRID vGPU graphics acceleration	11 or later	vSphere 6.0 or later

Prerequisites

- Complete the procedure described in [Upgrade Connection Servers in a Replicated Group](#).
- Perform the ESXi upgrade preparation tasks listed in the *VMware vSphere Upgrade Guide*.

Procedure

1 Upgrade ESXi hosts, cluster by cluster.

For instructions, see the *VMware vSphere Upgrade Guide*. If your clusters contain vSAN datastores, also see the chapter about upgrading the vSAN cluster, in the *Administering VMware vSAN* document. This chapter contains a topic about upgrading ESXi hosts.

If you have many clusters, this step could take several maintenance windows to complete. Upgrading ESXi hosts might include the following tasks:

- a Use VMware vSphere® vMotion® to move the virtual machines off of the ESXi host.
- b Put the host into maintenance mode.
- c Perform the upgrade.
- d Use vMotion to move the virtual machines back onto the host.
- e Perform post-upgrade tasks for ESXi hosts.

Every host must be a member of a cluster, as mentioned in the prerequisites.

2 If an upgraded host does not reconnect itself to vCenter Server, use vSphere Client to reconnect the host to vCenter Server.

3 If you use View Composer, after all ESXi hosts are upgraded, on the vCenter Server host, restart the View Composer service.

4 (Optional) Upgrade VMware® Tools™ and the virtual machines on all parent virtual machines, virtual machine templates, and virtual machines that host Horizon 7 server components such as Connection Server instances.

- a Plan for down time, as described in the *VMware vSphere Upgrade Guide*.
- b Update VMware Tools, and upgrade the virtual machine hardware for virtual machines that will be used as sources for remote desktops.

For step-by-step instructions if you plan not to use VMware vSphere® Update Manager™, see the chapter about upgrading virtual machines in the *VMware vSphere Virtual Machine Administration* document.

If you use VMware vSphere Update Manager, you can update VMware Tools and then the virtual hardware version in the correct order for all the virtual machines in a particular folder. See the *VMware vSphere Upgrade Guide*.

5 (Optional) If you use full-clone desktops, on each virtual machine, upgrade VMware Tools and the virtual hardware for virtual machines that will be used as sources for remote desktops.

For step-by-step instructions if you plan not to use VMware vSphere® Update Manager™, see the chapter about upgrading virtual machines in the *VMware vSphere Virtual Machine Administration* document.

If you use vSphere Update Manager, you can update VMware Tools and then the virtual hardware version in the correct order for all the virtual machines in a particular folder. See the *VMware vSphere Upgrade Guide*.

What to do next

Upgrade the agent software. See [Upgrade View Agent or Horizon Agent](#).

Upgrading Published and Virtual Desktops

7

Upgrade published desktops, virtual desktops and Horizon Agent, which runs inside the operating systems of virtual desktops or published desktops and Microsoft RDS hosts.

Important This chapter does not contain information about upgrading Horizon Agent on a Linux virtual machine. For this information, see *Setting Up Horizon 7 for Linux Desktops*.

This chapter includes the following topics:

- [Security-Related Requirements for Desktop Upgrade](#)
- [Upgrade RDS Hosts That Provide Session-Based Desktops](#)
- [Upgrade View Agent or Horizon Agent](#)
- [Upgrade View Composer Desktop Pools](#)
- [Upgrade Instant-Clone Desktop Pools](#)

Security-Related Requirements for Desktop Upgrade

RC4, SSLv3, and TLSv1.0 are disabled by default in Horizon 7 components. If you need to reenable RC4, SSLv3, or TLSv1.0 on a virtual desktop or published desktop, see "Older Protocols and Ciphers Disabled in Horizon 7" in the *Horizon 7 Security* document.

For complete information about the security features of View Agent, Horizon Agent, and Horizon Client, see the *Horizon Client and Agent Security* document.

Upgrade RDS Hosts That Provide Session-Based Desktops

On RDS hosts with Windows Server 2008 R2 or a later operating system, you can upgrade the View Agent or Horizon Agent software and edit pool settings so that the RDS host can provide remote desktops and remote Windows-based applications.

With VMware Horizon 6.0 and later releases, you can use Microsoft RDS hosts to provide remote applications, in addition to remote desktops. With this added functionality, the previously hidden server farm name is displayed in Horizon Administrator.

Prerequisites

- Verify that at least one Horizon Connection Server instance in the replicated group has been upgraded. Connection Server must be upgraded first so that the secure JMS pairing mechanism can work with Horizon Agent.
- Verify that the RDS host currently hosting remote desktops is running Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2. Windows Server 2008 (Terminal Services) was supported for earlier versions of Horizon 7 but is not a supported operating system for this release. If you do not have a supported Windows Server operating system, you must do a fresh installation rather than an upgrade. For a list of supported operating systems, see [Supported Operating Systems for Horizon Agent](#).
- Verify that the RDS Host role is installed in the operating system. See the procedure called "Install Remote Desktop Services on Windows Server 2008 R2" in the *Setting Up Published Desktops and Applications in Horizon 7* document.
- Familiarize yourself with the procedure for running the Horizon Agent installer. See the procedure called "Install Horizon Agent on a Remote Desktop Services Host," in *Setting Up Published Desktops and Applications in Horizon 7*, available by clicking the **Help** button in Horizon Administrator.
- Verify that you have logged off from all remote desktops and remote applications.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.

Procedure

- 1 In Horizon Administrator, edit the desktop pool settings for the pool to disable the pool.
Go to **Catalog > Desktop Pools**, select the pool, and click **Edit**.
- 2 On the RDS host, download and run the installer for the new version of Horizon Agent.
You can download the installer from the VMware Web site.
- 3 In Horizon Administrator, edit the farm settings and set the default display protocol to **PCoIP** or **VMware Blast**.
Go to **Resources > Farms**, select the farm, and click **Edit**.
You can also use a setting that allows the end user to choose the protocol. To use remote applications, the protocol must be PCoIP or VMware Blast. Remote applications are not supported with RDP.

- 4 In Horizon Administrator, edit the desktop pool settings for the pool to enable the pool.

This host can now provide remote applications in addition to remote desktops. In Horizon Administrator, if you go to **Catalog > Desktop Pools**, you see that the type of pool is **RDS Desktop Pool**. If you go to **Resources > Farms**, you see a farm ID in the list that corresponds to the pool ID.

What to do next

Upgrade the clients. See [Chapter 3 Upgrade the Client Application](#).

Upgrade View Agent or Horizon Agent

The strategy for upgrading the agent software depends on the type of desktop source.

Note To upgrade the operating system in a virtual machine desktop from Windows 8 to Windows 8.1, you must uninstall Horizon Agent, upgrade the operating system from Windows 8 to Windows 8.1, and then reinstall Horizon Agent. Alternatively, you can perform a fresh installation of Windows 8.1 and then install Horizon Agent.

This procedure provides an overview of the tasks you must perform to upgrade the agent software in virtual machines used as desktop sources. To complete some of these tasks, you might need the step-by-step instructions found in the vSphere Client online help or in *Setting Up Virtual Desktops in Horizon 7*, available by clicking the **Help** button in Horizon Administrator. To upgrade the agent software on a Terminal Services host or Microsoft RDS host, see [Upgrade RDS Hosts That Provide Session-Based Desktops](#). To upgrade the agent software on a Linux virtual machine, see the separate document, *Setting Up Horizon 7 for Linux Desktops*.

If you plan to deploy instant clones, you can use this procedure to create a parent virtual machine for an instant-clone desktop pool. When you upgrade Horizon Agent on a parent virtual machine, simply select the appropriate option for an instant-clone desktop pool.

Important The Horizon Agent installer now includes all components that were previously included in the Remote Experience Agent, which was part of the VMware Horizon™ View™ Feature Pack. To upgrade features that were installed with the Remote Experience Agent, you can simply run the Horizon Agent installer. This installer removes the Remote Experience Agent before performing the upgrade. If, for some reason, you decide to manually remove the Remote Experience Agent, be sure to do so before you run the installer for the new version of Horizon Agent.

Prerequisites

- Verify that at least one Connection Server instance in the replicated group has been upgraded. Connection Server must be upgraded first so that the secure JMS pairing mechanism can work with Horizon Agent.
- If you are upgrading ESXi hosts and virtual machines, complete the procedure described in [Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines](#).
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.

Procedure

- 1 If you plan to deploy instant clones or View Composer linked clones, upgrade the agent software on a parent virtual machine and create a desktop pool for testing purposes.

- a Download and run the new version of the Horizon Agent installer on a parent virtual machine.

You can download the installer from the VMware Web site.

- b Create a small desktop pool from this virtual machine.
- c Test a virtual machine desktop from the desktop pool to verify that all the usage scenarios function properly.

For example, create a desktop pool that contains one virtual machine desktop, and verify that you can use Horizon Client to log in to that desktop.

Step-by-step instructions for running the Horizon Agent installer and creating desktop pools appear in *Setting Up Virtual Desktops in Horizon 7*, available by clicking the **Help** button in Horizon Administrator.

Important If you are upgrading from View 5.1.x or earlier, and you use Sysprep, and your end users will connect USB devices to their remote desktops, you must follow the procedure described in the VMware Knowledge Base, at <http://kb.vmware.com/kb/2051801>. Otherwise, after you upgrade the agent software, the USB redirection feature might not work.

- 2 On the other parent virtual machines and virtual machine templates, download and run the installer for the new version of Horizon Agent.

Step-by-step instructions for running the Horizon Agent installer and creating desktop pools appear in *Setting Up Virtual Desktops in Horizon 7*, available by clicking the **Help** button in Horizon Administrator.

- 3 If you plan to create instant-clone or View Composer linked-clone desktop pools, take a snapshot of each upgraded parent virtual machine.

Use the new snapshot for creating an instant-clone or linked-clone desktop pool, or for recomposing an existing linked-clone desktop pool.

For instructions on taking snapshots, see the vSphere Client online help.

- 4 If you use full-clone desktops or other virtual machines that you added as individual desktops or as part of a manual pool, upgrade the agent software by using whatever third-party tools you usually use for software upgrades.

- 5 For automated and manual Windows 7 and 8 pools that are not instant-clone or linked-clone pools, to turn on the 3D rendering feature, edit the pool and power the virtual machine desktops off and on.

- a Configure the following pool settings:

- Set the pool to use the PCoIP display protocol or the VMware Blast display protocol.
- Set **Allow users to choose protocol** to **No**.
- Turn on the **3D Renderer** feature.

- b Power off each virtual machine and power it on again.

Restarting a virtual machine, rather than powering off and on, does not cause the setting to take effect.

- 6 If you use physical PCs or virtual machines as Microsoft RDS hosts, to provide remote desktops or applications, download and run the installer for the new version of Horizon Agent on these machines.

You can download the installer from the VMware Web site.

Important When you run the installer on a virtual machine RDS host, the **View Composer Agent** component is de-selected. Do not select this component during an upgrade. If you want to use this component to create an automated farm, which is a feature introduced with Horizon 6 version 6.2, uninstall the previous version of the agent software and then install the new version with the **View Composer Agent** component selected.

- 7 If you use physical PCs as desktop sources, download and run the installer for the new version of Horizon Agent on these physical machines.

You can download the installer from the VMware Web site.

- 8 Use a Horizon Client that has not been upgraded to verify that you can log in to the upgraded remote desktop sources with your old client software.

What to do next

If you use View Composer desktop pools, recompose or recreate the pools. See [Upgrade View Composer Desktop Pools](#).

Upgrade clients. See [Chapter 3 Upgrade the Client Application](#).

Upgrade View Composer Desktop Pools

Part of the final phase of a Horizon upgrade includes upgrading View Composer desktop pools.

Upgrading pools that were created with View Composer requires that you use a snapshot taken after upgrading Horizon Agent on the parent virtual machine.

Important If you use View Composer linked clones and you want to use the space reclamation feature available with vSphere 5.1 and later virtual machines, you must configure certain settings in View LDAP and in Horizon Administrator, in addition to performing the steps in this procedure. For a complete list of tasks, see [Tasks for Upgrading Desktop Pools to Use Space Reclamation](#).

Note If you are also upgrading the virtual hardware version, such as upgrading to virtual hardware version 8 or later, included with vSphere 5 or later, the snapshot of the upgraded parent virtual machine is used to upgrade the virtual hardware version of the rest of the virtual machines in the linked-clone pool.

Upgrading in this way, from one virtual hardware version (or compatibility level) to a higher version, is supported. You cannot, however, recompose linked clones to a lower hardware version than their current version. For example, you cannot recompose hardware version 8 clones to a parent virtual machine that is hardware version 7.

Prerequisites

- Complete the procedure described in [Upgrade View Composer](#).
- Complete the procedure described in [Upgrade Connection Servers in a Replicated Group](#).
- If you are also upgrading ESXi hosts and virtual machines, complete the procedure described in [Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines](#).

For information about the vSphere versions that are required for various new features, see [Table 6-1. Virtual Hardware Versions Required for Specific Features](#).

- Complete the procedure described in [Upgrade View Agent or Horizon Agent](#) for upgrading the agent in the parent virtual machine.

Important If you are upgrading from View 5.1.x or earlier, and you use Sysprep, and your end users will connect USB devices to their remote desktops, you must follow the procedure described in the VMware Knowledge Base, at <http://kb.vmware.com/kb/2051801>. Otherwise, after you upgrade the agent software, the USB redirection feature might not work.

- Plan maintenance windows carefully so that recreating and recomposing desktop pools will not overwhelm the storage array and ESXi hosts.

Procedure

- 1 If you disabled provisioning of new virtual machines in preparation for the upgrade, enable provisioning again.
- 2 To turn on the 3D rendering feature, edit the pool to configure the following settings:
 - Set the pool to use the PCoIP display protocol or the VMware Blast display protocol.
 - Set **Allow users to choose protocol** to **No**.
 - Turn on the **3D Rendering** feature.

- 3 To enable the space reclamation feature available with vSphere 5.1 virtual machines, in the **Advanced Storage** section of pool settings, select **Reclaim VM disk space**, and set the threshold for space reclamation to 1GB.
- 4 To enable View Storage Accelerator, available with vSphere 5.0 or later virtual machines, in the **Advanced Storage** section of pool settings, verify that the **Use View Storage Accelerator** check box is selected.

View Storage Accelerator can improve performance during boot storms and anti-virus scanning I/O storms by allowing ESXi hosts to cache common virtual machine disk data.

Important This feature is turned on by default. View Storage Accelerator requires 1GB of RAM per ESXi host.

- 5 Use the snapshot you created after upgrading the parent virtual machine to recompose desktop pools.
- 6 If you changed the **Refresh OS disk on logoff** setting for a pool to **Never** in preparation for the upgrade, change the setting back to reflect the appropriate refresh policy.
- 7 If you canceled any refresh or recompose operations for any desktop pools, schedule the tasks again.

What to do next

Upgrade the clients. See [Chapter 3 Upgrade the Client Application](#).

Perform the tasks listed in [Chapter 9 Post-Upgrade Tasks to Enable New Features in Your Horizon Setup](#) that apply to your setup.

Upgrade Instant-Clone Desktop Pools

If you upgrade vCenter Server to use vSphere 6.7, you must also upgrade the instant-clone desktop pools.

Prerequisites

- Complete the system requirements for an upgrade to Horizon 7 version 7.5 or later.
- Complete procedures described in [Upgrading Horizon Connection Server](#).
- Complete the procedure described in [Upgrade View Agent or Horizon Agent](#) for upgrading the agent in the parent VM.
- Complete the prerequisites listed in the *VMware vSphere Upgrade Guide*, using the version of the guide that corresponds to the version of vSphere that you plan to upgrade to.

Note If you upgrade vCenter Server to vSphere 6.7, then all or some of the ESXi hosts in the cluster must be upgraded to vSphere 6.7. Else, the instant-clone desktop pools might not work correctly.

- Identify the ESXi hosts that you plan to upgrade and verify that you leave enough hosts online for existing desktop pools.

Procedure

- 1 Take a snapshot of the parent VM on which you upgrade Horizon Agent to Horizon 7 version 7.5 or later. This snapshot is the master image for instant clones.
- 2 Set the Storage Distributed Resource Scheduler (DRS) migration threshold to 3 in the cluster.
- 3 Disable the instant-clone desktop pools.
- 4 Upgrade vCenter Server to vSphere 6.7.
- 5 To put the hosts that you plan to upgrade into maintenance mode, choose one of the following options.
 - Put the host directly into maintenance mode from vSphere Web Client then upgrade the host to vSphere 6.7. After the upgrade completes, use vSphere Web Client to exit maintenance mode.
 - Use the `icmaint.cmd` utility to mark a host for maintenance with the **ON** option. Marking a host for maintenance, deletes the master images, which are the parent VMs in vCenter Server from the ESXi host. Put the host into maintenance mode and upgrade to vSphere 6.7 ESXi. After the upgrade completes, exit the host from maintenance mode. Then, use the `icmaint.cmd` to unmark the host for maintenance with the **OFF** option.
- 6 Enable the instant-clone desktop pools.
- 7 Perform a push-image operation for each instant-clone desktop pool that uses the new snapshot.

Only the hosts that are upgraded to vSphere 6.7 ESXi are used for provisioning. The instant clones created during the push-image operation might be migrated to other hosts that are not yet on vSphere 6.7.
- 8 Verify that all hosts in the cluster are upgraded to vSphere 6.7.
- 9 If you upgrade the parent VM from a previous version to be compatible with ESXi 6.7 and later (VM version 14), then upgrade VMware Tools on the parent VM. You must take a new snapshot of the parent VM, which is the master image for instant clones and perform a push-image operation on all the instant-clone desktop pools that used the previous version of this master image.
- 10 If the Virtual Distributed Switch (vDS) is upgraded, power on the parent VM on to verify that there are no network issues. Following a vDS upgrade, you must take a new snapshot of the parent VM and perform a push-image operation on all the instant-clone desktop pools.

Upgrade Horizon 7 Cloud Connector Virtual Appliance

8

Upgrade to the latest version of the Horizon 7 Cloud Connector virtual appliance to bridge your Horizon 7 pods with the latest VMware Horizon Cloud Service features.

Note Proxy SSL configuration is not supported during an upgrade of the Horizon 7 Cloud Connector virtual appliance.

Prerequisites

- Install and deploy the Horizon 7 Cloud Connector virtual appliance. See the *Horizon 7 Installation* document.
- Verify that the new Horizon 7 Cloud Connector virtual appliance and the existing Horizon 7 Cloud Connector virtual appliance that needs the upgrade are in the same network so that the new virtual appliance can establish an SSH communication with the existing virtual appliance.
- Use vSphere Web Client to take a snapshot of the existing Horizon 7 Cloud Connector virtual appliance.
- Obtain the static IP address, DNS address, gateway address, and subnet mask for the Horizon 7 Cloud Connector virtual appliance.
- When an Active Directory domain is already joined, verify that you have the credentials for an Active Directory account in that domain that has access permissions.
- Add the FQDN of the vCenter Server to the `/etc/hosts` file on the Horizon 7 Cloud Connector virtual appliance.

Procedure

- 1 In vSphere Web Client, power on the existing Horizon 7 Cloud Connector appliance.
The Horizon 7 Cloud Connector appliance user interface IP address appears.

- 2 If you are upgrading from version 1.0 of the Horizon 7 Cloud Connector virtual appliance, login as the root user from vCenter Server to the existing Horizon 7 Cloud Connector virtual appliance and enter the `chage -E -1 -M -1 tomcat8` command.

For example, enter the following command: `root@example.com [~]# chage -E -1 -M -1 tomcat8`

Note This step is not required for version 1.1 and later of the Horizon 7 Cloud Connector virtual appliance.

- 3 In a Web browser, enter the Horizon 7 Cloud Connector virtual appliance IP address to log in to the Horizon 7 Cloud Connector user interface.

Use your My VMware account credentials to log in. This step verifies that the existing Horizon Cloud connection was successfully configured with the Connection Server that is hosted on-premises.

- 4 Deploy the latest version of the Horizon 7 Cloud Connector virtual appliance and use your My VMware account credentials to log in.

Note If the environment associated with the My VMware account has a joined Active Directory domain, the Active Directory login window appears and you must log in with Active Directory credentials.

- 5 Connect the latest version of the Horizon 7 Cloud Connector appliance with the Connection Server instance on-premises. In the **Connect to Horizon 7 Connection Server** box, enter the FQDN of the Connection Server that is hosted on-premises, and click **Connect**.
- 6 Click the check box to verify the thumbprint certificate for the Connection Server.

Note This verification is skipped if the Connection Server has a valid Root CA certificate.

- 7 Enter the domain name, user name, and password for the Connection Server and click **Connect**.

Note For better auditing of Horizon 7 Cloud Connector actions, use a unique user name and password for the Connection Server.

- 8 Click **Upgrade** in the dialog box.
- 9 In the **Old Cloud Connector address** text box, enter the IP address of the earlier Horizon 7 Cloud Connector virtual appliance and then click **Connect**.
- 10 Click the check box to verify the thumbprint for the SSH connection.
- 11 Click **Upgrade**.

The Horizon 7 pod is successfully upgraded and paired with the VMware Horizon Cloud Service.

- 12 On the final wizard page, click **Configure Virtual Center** and specify vCenter Server settings.

This configuration enables support for Horizon Cloud to run maintenance actions on the virtual appliance, as needed for successful service operations.

- a Enter the FQDN of the vCenter Server, and click **Get Certificate**. After the certificate information appears, select **I have verified the above certificate and would like to continue**.
- b Under **Horizon Cloud Connector vCenter Server Credentials**, enter the user name and password for vCenter Server.
- c Under **Additional Static IP Details for Cloud Connector upgrade**, enter the static IP, gateway, subnet mask, and DNS information that you gathered earlier for the Horizon 7 Cloud Connector virtual appliance.
- d Click **Save**.

Static IP and Proxy Configuration for the Horizon 7 Cloud Connector Virtual Appliance

Information about the static IP and proxy settings for the Horizon 7 Cloud Connector virtual appliance is saved in certain container files.

Static IP Storage

The static IP address of the Horizon 7 Cloud Connector virtual appliance is saved in the `–/opt/container-data/cc-settings/ip.conf` file and is shared with containers running inside the appliance.

For example, the static IP information might appear in the file as follows.

```
cc.address=10.117.163.20
```

Proxy Storage

The proxy settings of the Horizon 7 Cloud Connector virtual appliance are stored in the `–/opt/container-data/cc-settings/proxy.conf` and are shared with containers running inside the appliance.

For example, the proxy information might appear in the file as follows.

```
proxyHost=null
proxyPort=0
proxySsl=false
proxyUsername=null
proxyPassword=
noProxyFor=null
```

Update the Static IP for the Horizon 7 Cloud Connector Virtual Appliance

If you update the static IP address for the Horizon 7 Cloud Connector virtual appliance, you must also perform some additional steps. You must manually reconfigure the container settings file and then send the new static IP information to all desktops associated with the paired Horizon 7 pod.

Prerequisites

Configure a new static IP address for the Horizon 7 Cloud Connector virtual appliance, and join the appliance to Active Directory.

Procedure

- 1 Edit the `cc.address` line in the `–/opt/container–data/cc–settings/ip.conf` file, as shown in the following example.

```
cc.address=[new static IP address]
```

- 2 To send the new static IP address to all running Horizon 7 desktops, run the following command.

```
docker exec csms /bin/bash –c "cd /usr/local/csms; ./scripts/address_changed.sh"
```

Troubleshoot the Horizon 7 Cloud Connector Virtual Appliance Upgrade

The earlier version of the Horizon 7 Cloud Connector virtual appliance is disabled only at the end of the upgrade process. If there is any upgrade issue, you can roll back the upgrade to the earlier version of the Horizon 7 Cloud Connector virtual appliance.

Note When you perform any troubleshooting task, do not unplug the latest deployed version of the Horizon 7 Cloud Connector appliance.

Procedure

- 1 If the upgrade fails and the earlier version of the Horizon 7 Cloud Connector virtual appliance is still accessible, you can continue to use this version of the virtual appliance. After you check the log files and verify the configuration information of the new Horizon 7 Cloud Connector virtual appliance, you can perform the upgrade task again.

- 2 If the upgrade fails and the earlier version of the Horizon 7 Cloud Connector virtual appliance is not accessible, perform these steps:
 - a Power off the new Horizon 7 Cloud Connector virtual appliance.
 - b Revert the existing Horizon 7 Cloud Connector virtual appliance to the virtual appliance snapshot taken prior to the upgrade. Verify that the Horizon 7 Cloud Connector virtual appliance is accessible from the Web browser and displays the paired status.
 - c Perform the upgrade task to deploy the latest version of the Horizon 7 Cloud Connector appliance again . If the issue persists, contact VMware Support.

Post-Upgrade Tasks to Enable New Features in Your Horizon Setup

9

After you finish upgrading the servers, virtual machines, and agent software for desktop and application pools, you can configure your setup to take advantage of certain new features.

In addition to the tasks described in the topics in this chapter, if applicable, you can use Horizon Administrator to edit advanced storage options for desktop pools, and change the scope of transparent page sharing. By default, as a security precaution, memory sharing is not allowed among virtual machines on an ESXi host. For more information, see the topic called "Modifying Settings in an Existing Desktop Pool" in the *Horizon 7 Administration* document.

This chapter includes the following topics:

- [Change the JMS Message Security Mode to Enhanced](#)
- [Tasks for Upgrading Desktop Pools to Use Space Reclamation](#)
- [Upgrade Tasks If You Use VMware vSAN Datastores](#)
- [Configure the VMware Horizon Web Portal Page for End Users](#)

Change the JMS Message Security Mode to Enhanced

When you upgrade, the existing JMS message security mode setting used for the previous version is retained. Beginning with Horizon 6 version 6.1, you can use Horizon Administrator to change this setting to **Enhanced**.

This procedure shows how to use Horizon Administrator to change the message security mode to **Enhanced** and monitor the progress of the change on all Horizon components. You can alternatively use the `vdmutil` command-line utility to change the mode and monitor progress. See the *Horizon 7 Administration* document.

Note With Horizon 6 version 6.2 and later releases, you can use Access Point appliances instead of Horizon security servers. Access Point uses a standard HTTP(S) protocol for communication with Connection Server. JMS, IPsec, and AJP13 are not used.

To use Access Point appliances instead of Horizon security servers, you must upgrade the Connection Server instances to version 6.2 or later before installing and configuring the Access Point appliances to point to the Connection Server instances or the load balancer that fronts the instances. For more information, see *Deploying and Configuring Unified Access Gateway*.

Prerequisites

Verify that you have upgraded all Horizon Connection Server instances, security servers, and Horizon desktops to Horizon 6 version 6.1 or a later release. View components that predate Horizon 6 version 6.1 cannot communicate with a Connection Server 6.1 instance that uses Enhanced mode.

Procedure

- 1 Configure back-end firewall rules to allow security servers to send JMS traffic on port 4002 to Connection Server instances.
- 2 In Horizon Administrator, go to **View Configuration > Global Settings**, and on the **Security** tab, set **Message security mode** to **Enhanced**.
- 3 Manually restart the VMware Horizon Message Bus Component service on all Connection Server hosts in the pod, or restart the Connection Server instances.

After the services are restarted, the Connection Server instances reconfigure the message security mode on all desktops and security servers, changing the mode to **Enhanced**.

- 4 To monitor the progress in Horizon Administrator, go to **View Configuration > Global Settings**.

On the **Security** tab, the **Enhanced Security Status** item will show **Enhanced** when all components have made the transition to Enhanced mode.

When servers communicate with clients, servers will configure clients to use enhanced message security mode.

Tasks for Upgrading Desktop Pools to Use Space Reclamation

Starting with vSphere 5.1, Horizon 7 creates linked-clone virtual machines in an efficient disk format that allows ESXi hosts to reclaim unused disk space in the linked clones. Upgrading pools to use this feature

involves changing settings in vCenter Server, View LDAP, and pool settings and then recomposing the pool.

Note The space reclamation feature is not supported if your virtual machine desktops are hosted on vSAN datastores or Virtual Volumes datastores.

Although the space reclamation feature reduces the amount of disk space used for a virtual machine, it can reclaim only space that is not used. This feature cannot reclaim disk space created by virtual machines that have not been optimized. To optimize an operating system image, you can turn off Windows services such as the indexer service, the defragmenter service, and restore points. For details, see the topics "Optimize Windows Guest Operating System Performance," "Optimize Windows 7 and Windows 8 Guest Operating System Performance," and "Optimizing Windows 7 and Windows 8 for Linked-Clone Desktops," in *Setting Up Virtual Desktops in Horizon 7*.

Important Because this procedure involves recomposing the desktop pool, any changes that end users have made to the operating system disk will be lost.

- 1 If all vCenter Server instances and ESXi hosts for the pool are not at VMware vSphere 5.1 or later, upgrade them to 5.1 or later.

For instructions, see the *VMware vSphere Upgrade Guide*.

- 2 If all virtual machine desktops in the pool are not VMware vSphere 5.1 (virtual hardware version 9) or later virtual machines, upgrade them.

- In the parent virtual machine, upgrade VMware Tools to the latest VMware vSphere 5.1 or later version, and upgrade the virtual machine to the latest version, which must be virtual hardware version 9 or later.

For instructions, see the *VMware vSphere Upgrade Guide*.

- Take a snapshot of the parent virtual machine. For instructions on taking snapshots, see the vSphere Client online help.
- Use the snapshot of the parent virtual machine you just created to recompose the desktop pool. For instructions on recomposing pools, click the **Help** button in Horizon Administrator.

Recomposing the pool from a snapshot of an upgraded virtual machine is just one method of upgrading all virtual machines in a linked-clone pool. You can also upgrade the virtual machines one by one.

- 3 Upgrade the disk format used for the virtual machines.

- On the Connection Server host, use ADSIEdit to navigate to the server group that corresponds to the pool, and change the value in the **pae-UseSeSparseFormat** field from **0** to **1**.
- Recompose the desktop pool.

- 4 Use Horizon Administrator to edit the vCenter Server settings, navigate to the **Storage** tab, and select **Reclaim VM disk space**.

For instructions on editing server settings, click the **Help** button in Horizon Administrator.

- 5 Use Horizon Administrator to edit the pool settings, navigate to the **Advanced Storage** section, select **Reclaim VM disk space**, and set the threshold for space reclamation to 1GB.

Upgrade Tasks If You Use VMware vSAN Datastores

Starting with vSphere 5.5 Update 1, you can use the vSAN feature for high-performance storage and policy-based management.

With vSAN, the locally attached physical storage disks available on a cluster of vSphere hosts are aggregated into one virtual datastore. You specify this datastore when creating a desktop pool, and the various components, such as virtual machine files, replicas, user data, and operating system files, are placed on the appropriate solid-state drive (SSD) disks or direct-attached hard disks (HDDs).

Horizon 7 defines virtual machine storage requirements, such as capacity, performance, and availability, in the form of default storage policy profiles, depending on the pool settings used. Storage is provisioned and automatically configured according to the assigned policies.

Note The space reclamation feature is not supported if your virtual machine desktops are hosted on vSAN datastores.

Upgrade from a Non-vSAN Datastore to a vSAN Datastore

Upgrading pools to use VMware vSAN datastores involves changing a pool setting and then rebalancing the pool.

The tasks outlined in this procedure describe upgrading from a non-vSAN datastore to a vSAN datastore. Upgrading from vSAN datastore on a vSphere 5.5 or earlier cluster (a Tech Preview feature) is not supported.

Important Because this procedure involves recomposing the desktop pool, any changes that end users have made to the operating system disk will be lost.

Prerequisites

- Verify that all ESXi hosts in the cluster used for the pool are upgraded to 5.5 Update 1 or later and that they meet the system requirements for the vSAN feature. VMware recommends that you upgrade to vSphere 6.0 or later because the vSAN feature available with vSphere 6.0 and later releases contains many performance improvements over the feature that was available with vSphere 5.5 Update 1. With vSphere 6.0 this feature also has broader HCL (hardware compatibility) support.

For information about upgrades, see [Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines](#) and see the *VMware vSphere Upgrade Guide*. For information about vSAN requirements and upgrades, see the *Administering VMware vSAN* document.

- In vCenter Server, verify that the following privileges are added to the Composer role:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

Procedure

- 1 Use vCenter Server 5.5 Update 1 or later to enable vSAN for the vSphere cluster.

For more information, see the *vSphere Storage* document.

- 2 Upgrade the desktop pool to the latest version, as described in [Upgrade View Composer Desktop Pools](#).

This process includes installing the latest version of Horizon Agent on the parent virtual machine and taking a snapshot.

- 3 Recompose the pool on the non-vSAN datastore using the snapshot of the parent virtual machine you just created.

For instructions on recomposing pools, click the **Help** button in Horizon Administrator.

- 4 Edit the pool settings of the newly upgraded desktop pool to enable the **Use VMware Virtual SAN** pool setting, change the datastore from a non-vSAN datastore to a vSAN datastore, and use the **Rebalance** command.

For instructions on editing server settings and using the **Rebalance** command, click the **Help** button in Horizon Administrator.

Upgrade from vSAN Disk Format Version 1

After upgrading from VMware vSphere 5.5 Update 1 to vSphere 6.0 or a later release, you must also upgrade the vSAN disk format.

VMware recommends that you upgrade to vSphere 6.0 or later because the vSAN feature available with vSphere 6.0 and later releases contains many performance improvements over the feature that was available with vSphere 5.5 Update 1. With vSphere 6.0 this feature also has broader HCL (hardware compatibility) support.

Important This procedure describes an upgrade process for vSAN if you currently have desktop pools on vSAN datastores available with vSphere 5.5 Update 1 or a later update release. If your desktop pools do not currently use vSAN datastores, see [Upgrade from a Non-vSAN Datastore to a vSAN Datastore](#).

Upgrading a VMware vSAN datastore is a multi-phase process that includes upgrading the vSphere software on each ESXi host, and then upgrading the disk format, one disk group at a time. An entire chapter of the vSphere 6 document *Administering VMware vSAN* is devoted to the upgrade process. The steps in the following procedure outline the order of tasks to do at the ESXi host level, in vCenter Server, and at the desktop pool level, in View Administrator.

Prerequisites

- Verify that your desktop pools are using View Agent 6.0 or a later version. If your virtual machines use View Agent 5.3.x on vSAN datastores, see [Upgrade from Horizon View 5.3.x on a vSAN Datastore](#).

- In vCenter Server, verify that the following privileges are added to the Composer role:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

- Familiarize yourself with the vSAN upgrade process. See the chapter about upgrading vSAN in the *Administering VMware vSAN* document, available at <https://docs.vmware.com/en/VMware-vSAN/index.html>.

Procedure

- 1 Upgrade vCenter Server and your ESXi hosts to vSphere 6 or later, as described in the chapter about upgrading the vSAN cluster in the *Administering VMware vSAN* document, available in the vSphere 6.0 documentation center.

At this point, the desktop pool is still using vSAN disk format 1, and the virtual machines and VMware Tools have not yet been upgraded to vSphere 6.0 virtual hardware version 11.

- 2 Upgrade the desktop pool to the latest version, as described in [Upgrade View Agent or Horizon Agent](#) and [Upgrade View Composer Desktop Pools](#).

This process includes installing the latest version of Horizon Agent on the parent virtual machine, virtual machine template, or full-clone virtual machines in the pool. For linked-clone pools, the process also includes taking a snapshot and recomposing the pool.

The virtual machines in the desktop pool now have View Agent 6.1 or later installed, and the virtual machines still reside on vSAN datastores available with vSphere 5.5 Update 1. At this point, the desktop pool is using vSAN disk format 1.

- 3 Upgrade the vSAN disk format version from version 1 to version 2.

For complete instructions, see the topic "Upgrading the vSAN Disk Format," in the upgrade chapter of the *Administering VMware vSAN* document, available at <https://docs.vmware.com/en/VMware-vSAN/index.html>.

You can use the command-line RVC tool for this upgrade, or, if you have vSphere 6 Update 1, you can use vSphere Web Client. Ruby vSphere Console (RVC) is a Ruby-based command-line console for VMware ESXi hosts and vCenter Server. RVC is included in both the Windows and Linux versions of vCenter Server. For detailed information about using the RVC commands, see the *RVC Command-line Reference Guide*.

- 4 After the disks are upgraded for all the ESXi hosts in the cluster, on the parent virtual machine, virtual machine template, or full-clone virtual machines in the pool, complete the following tasks in the following order.
 - a If the parent virtual machine is on a vSAN datastore, delete all snapshots.
 The virtual machine cannot start using the new snapshot format available with vSAN disk format 2 until all previous redo log-based snapshots are deleted. If the virtual machine is not on a vSAN datastore, you are not required to delete the snapshots.
 - b Upgrade the virtual machine hardware to version 11 and upgrade VMware Tools.
- 5 For linked-clone pools, take a new snapshot and recompose the desktop pool using the new snapshot.

The desktop pool is now using vSAN disk format 2.

Upgrade from Horizon View 5.3.x on a vSAN Datastore

Horizon 6.0 introduced some new default storage policies for vSAN. These policies are not automatically applied to existing virtual machine desktops created on vSAN by Horizon 7 5.3.x after the desktop pool is upgraded.

In addition, when you upgrade from Horizon 7 5.3.x, the **Use VMware Virtual SAN** pool setting will not automatically be enabled, even if the pool is on a vSAN datastore. You have the following upgrade options:

- If you continue to use VMware vSphere 5.5 Update 1, after upgrading, continue to use the default storage policies that were used with Horizon 7 5.3.x. If you choose this option, edit the pool settings so that **Use VMware Virtual SAN** is enabled.
- Use the procedure described in this topic so that the desktop pool uses the new default storage policies. This procedure involves rebalancing the desktop pool to a non-vSAN datastore and then upgrading and rebalancing back to the vSAN datastore.

Important The tasks outlined in this procedure describe upgrading from a Horizon 7 5.3.x desktop pool using a vSAN datastore on a VMware vSphere 5.5 Update 1 cluster. Upgrading from vSAN datastore on a VMware vSphere 5.5 or earlier cluster (a Tech Preview feature) is not supported.

Also, because this procedure involves recomposing the desktop pool, any changes that end users have made to the operating system disk will be lost.

Prerequisites

- Verify that all virtual machines in the pool are VMware vSphere 5.5 Update 1 or later virtual machines. VMware recommends that you upgrade to VMware vSphere 6.0 or later because the vSAN feature available with vSphere 6.0 and later releases contains many performance improvements over the feature that was available with vSphere 5.5 Update 1. With vSphere 6.0 this feature also has broader HCL (hardware compatibility) support.

For information about upgrades, see [Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines](#) and see the *VMware vSphere Upgrade Guide*. For information about vSAN requirements and upgrades, see the *Administering VMware vSAN* document.

- In vCenter Server, verify that the following privileges are added to the Composer role:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

Procedure

- 1 Edit the pool settings of the desktop pool to change the datastore from a vSAN datastore to a non-vSAN datastore, and use the **Rebalance** command.

For instructions on editing server settings and using the **Rebalance** command, click the **Help** button in View Administrator.

- 2 Upgrade the desktop pool to the latest version, as described in [Upgrade View Composer Desktop Pools](#).

This process includes installing the latest version of Horizon Agent on the parent virtual machine and taking a snapshot.

- 3 Recompose the pool on the non-vSAN datastore using the snapshot of the parent virtual machine you just created.

For instructions on recomposing pools, click the **Help** button in View Administrator.

- 4 Edit the pool settings of the newly upgraded desktop pool to change the datastore from a non-vSAN datastore to a vSAN datastore, and use the **Rebalance** command.

What to do next

If you upgraded your virtual machines to VMware vSphere 6.0, to upgrade to using vSAN 2 rather than vSAN 1, see [Upgrade from vSAN Disk Format Version 1](#).

Configure the VMware Horizon Web Portal Page for End Users

You can configure this Web page to show or hide the icon for downloading Horizon Client or the icon for connecting to a remote desktop through HTML Access. You can also configure other links on this page.

By default, the web portal page shows both an icon for downloading and installing the native Horizon Client, and an icon for connecting through HTML Access. The download link used is determined from the default values defined in the `portal-links-html-access.properties` file.

In some cases, however, you might want to have the links to point to an internal Web server, or you might want to make specific client versions available on your own server. You can reconfigure the portal page to point to a different download URL by modifying the contents of the `portal-links-html-access.properties` file. If that file is unavailable or is empty, and the `oslinks.properties` file exists, the `oslinks.properties` file is used to determine the link value for the installer file.

The `oslinks.properties` file is installed in the `installation-directory\VMware\VMware View\Server\broker\webapps\portal\WEB-INF` folder. If this file is missing during the HTML Access session, the download link will direct users to `https://www.vmware.com/go/viewclients` by default. The file contains the following default values:

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaip1jfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

You can make installer links for specific client operating systems in either the `portal-links-html-access.properties` or `oslinks.properties` file. For example, if you browse to the portal page from a Mac OS X system, the link for the native Mac OS X installer appears. For Windows or Linux clients, you can make separate links for 32-bit and 64-bit installers.

Procedure

- 1 On the Connection Server host, open the `portal-links-html-access.properties` file with a text editor.

The location of this file is `CommonAppDataFolder\VMware\VDM\portal\portal-links-html-access.properties`. For Windows Server 2008 operating systems, the `CommonAppDataFolder` directory is `C:\ProgramData`. To display the `C:\ProgramData` folder in Windows Explorer, you must use the Folder Options dialog box to show hidden folders.

If the `portal-links-html-access.properties` file does not exist and the `oslinks.properties` file does, open the `<installation-directory>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties` file to modify the URLs to use for downloading specific installer files.

Note Customizations for Horizon 7 5.x and earlier releases resided in the `portal-links.properties` file, which is located in the same `CommonAppDataFolder\VMware\VDM\portal\` directory as the `portal-links-html-access.properties` file.

2 Edit the configuration properties to set them appropriately.

By default, both the installer icon and the HTML Access icon are enabled and a link points to the client download page on the VMware Web site. To disable an icon, which removes the icon from the Web page, set the property to `false`.

Note The `oslinks.properties` file can only be used to configure the links to the specific installer files. It does not support the other options listed below.

Option	Property Setting
Disable HTML Access	<code>enable.webclient=false</code> If this option is set to <code>false</code> but the <code>enable.download</code> option is set to <code>true</code> , the user is taken to a Web page for downloading the native Horizon Client installer. If both options are set to <code>false</code> , the user sees the following message: "Contact your local administrator for instructions on accessing this Connection Server."
Disable downloading Horizon Client	<code>enable.download=false</code> If this option is set to <code>false</code> but the <code>enable.webclient</code> option is set to <code>true</code> , the user is taken to the HTML Access login Web page. If both options are set to <code>false</code> , the user sees the following message: "Contact your local administrator for instructions on accessing this Connection Server."
Change the URL of the Web page for downloading Horizon Client	<code>link.download=https://url-of-web-server</code> Use this property if you plan to create your own Web page.

Option	Property Setting
Create links for specific installers	<p>The following examples show full URLs, but you can use relative URLs if you place the installer files in the downloads directory, which is under the C:\Program Files\VMware\VMware View\Server\broker\webapps\ directory on Connection Server, as described in the next step.</p> <ul style="list-style-type: none"> ■ General link to download installer: <div data-bbox="671 411 1422 464" style="background-color: #f0f0f0; padding: 5px;"> <code>link.download=https://server/downloads</code> </div> ■ 32-bit Windows installer: <div data-bbox="671 527 1422 600" style="background-color: #f0f0f0; padding: 5px;"> <code>link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe</code> </div> ■ 64-bit Windows installer: <div data-bbox="671 663 1422 737" style="background-color: #f0f0f0; padding: 5px;"> <code>link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe</code> </div> ■ Windows Phone installer: <div data-bbox="671 800 1422 873" style="background-color: #f0f0f0; padding: 5px;"> <code>link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx</code> </div> ■ 32-bit Linux installer: <div data-bbox="671 936 1422 1010" style="background-color: #f0f0f0; padding: 5px;"> <code>link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle</code> </div> ■ 64-bit Linux installer: <div data-bbox="671 1073 1422 1146" style="background-color: #f0f0f0; padding: 5px;"> <code>link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle</code> </div> ■ Mac OS X installer: <div data-bbox="671 1209 1422 1283" style="background-color: #f0f0f0; padding: 5px;"> <code>link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg</code> </div> ■ iOS installer: <div data-bbox="671 1346 1422 1419" style="background-color: #f0f0f0; padding: 5px;"> <code>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</code> </div> ■ Android installer: <div data-bbox="671 1482 1422 1556" style="background-color: #f0f0f0; padding: 5px;"> <code>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</code> </div> ■ Chrome OS installer: <div data-bbox="671 1619 1422 1692" style="background-color: #f0f0f0; padding: 5px;"> <code>link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</code> </div>
Change the URL for the Help link in the login page	<p><code>link.help</code></p> <p>By default, this link points to a help system hosted on the VMware Web site. The Help link appears at the bottom of the login page.</p>

- 3 To have users download installers from a location other than the VMware Web site, place the installer files on the HTTP server where the installer files will reside.

This location must correspond to the URLs you specified in the `portal-links.html-access.properties` file or the `oslinks.properties` file from the previous step. For example, to place the files in a `downloads` directory on the Connection Server host, use the following path:

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

The links to the installer files could then use relative URLs with the format `/downloads/client-installer-file-name`.

- 4 Restart the Horizon Web Component service.

Upgrading vSphere Components Separately in a Horizon 7 Environment

10

If you upgrade vSphere components separately from Horizon 7 components, you must back up some Horizon 7 data and reinstall some Horizon 7 software.

Instead of performing an integrated upgrade of Horizon 7 and vSphere components, you can choose to first upgrade all Horizon 7 components and then upgrade vSphere components, or the reverse. You might also upgrade only vSphere components when a new version or update of vSphere is released.

When you upgrade vSphere components separately from Horizon 7 components, you must perform the following additional tasks:

- 1 Before you upgrade vCenter Server, back up the vCenter Server database and the View Composer database.
- 2 Before you upgrade vCenter Server, back up the Horizon LDAP database from a Horizon Connection Server instance by using the `vdmexport.exe` utility.

For instructions, see the *Horizon 7 Administration* document. If you have multiple instances of Connection Server in a replicated group, you need to export the data from only one instance.

- 3 If you use View Composer, after you upgrade all ESXi hosts that are managed by a particular vCenter Server instance, restart the View Composer service on that host.
- 4 After you upgrade VMware Tools in virtual machines that are used as remote desktops, reinstall Horizon Agent.

Reinstalling Horizon Agent guarantees that the drivers in the virtual machine remain compatible with the other Horizon 7 components.

Step-by-step instructions for running the Horizon Agent installer appear in the *Setting Up Virtual Desktops in Horizon 7* document.